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 ANTHEM BLUE CROSS BLUE SHIELD

Report Number 1A-10-62-16-003
August 15, 2016

EXECUTIVE SUMMARY

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

Report No. 1A-10-62-16-003 **August 15, 2016**

Background
Anthem Blue Cross Blue Shield (Anthem) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

Why Did We Conduct the Audit?
The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Anthem's information technology (IT) environment. This engagement was a follow-up audit where we performed test work that we were restricted from completing during a prior audit of Anthem (Report No. 1A-10-00-13-012). At the time of the previous audit Anthem was known as WellPoint, Inc.

What Did We Audit?
The scope of this audit centered on the information systems used by Anthem to process and store data related to 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 Anthem determined that:

- Anthem has implemented an incident response and network security program. Anthem has also implemented preventative controls at the network perimeter and performs security event monitoring throughout the network. However, we noted several areas of concern related to Anthem's network security controls:
  - Anthem's computer server and database inventories revealed that Anthem has numerous servers running unsupported versions of operating systems.
  - Our vulnerability assessment identified numerous servers containing vulnerabilities such as missing patches, noncurrent software, and weak configuration settings. The vast majority of the servers containing vulnerabilities were inherited from a separate company that was recently acquired by Anthem. These servers were migrated into Anthem's network before they were fully integrated into Anthem's vulnerability management, patching, and configuration management programs.
- Anthem has developed formal configuration management policies, has documented security configuration settings for its operating platforms, and performs routine configuration compliance auditing.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
Anthem	**Anthem Blue Cross Blue Shield**
BCBS	**Blue Cross Blue Shield**
BCBSA	**Blue Cross Blue Shield Association**
CFR	**Code of Federal Regulations**
DO	**Director's Office**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Systems Control 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**
Plan	**Anthem Blue Cross Blue Shield**

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. Network Security 4
B. Configuration Management 9

IV. **MAJOR CONTRIBUTORS TO THIS REPORT** 11

APPENDIX: Anthem Blue Cross Blue Shields's July 7, 2016 response to the draft audit report, issued April 27, 2016.

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) claims by Anthem Blue Cross Blue Shield (Anthem or Plan).

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 (the 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.

The Blue Cross Blue Shield Association (BCBSA), on behalf of participating Blue Cross and Blue Shield (BCBS) plans, has entered into a Government-wide Service Benefit Plan contract (CS 1039) with OPM to provide a health benefit plan authorized by the FEHB Act. The Association delegates authority to participating local BCBS plans throughout the United States, such as Anthem, to process the health benefit claims of its federal subscribers.

The Association has established a Federal Employee Program (FEP) Director's Office (DO) in Washington, D.C. to provide centralized management for the Service Benefit Plan. The FEP DO coordinates the administration of the contract with the Association, member BCBS plans, and OPM.

All Anthem personnel that worked with the auditors were helpful and open to ideas and suggestions. 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 Anthem's information technology (IT) environment. We accomplished these objectives by reviewing IT security controls related to Anthem's network security and configuration management.

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 Anthem'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 Anthem'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.

This engagement was a follow-up audit where we performed test work that we were restricted from completing during a prior audit of Anthem. (Report No. 1A-10-00-13-012). At the time of the previous audit Anthem was known as WellPoint, Inc. All recommendations from the prior audit have been closed. The business processes reviewed are primarily located in Anthem's Indianapolis, Indiana facility.

The on-site portion of this audit was performed in November of 2015. 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 controls in place at Anthem as of April 2016.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Anthem. 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 Anthem's business structure and environment;
- Performed a risk assessment of Anthem's information systems environment and applications, and prepared an audit program based on the assessment and the 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 to evaluating Anthem'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;
- Information Technology Governance Institute's COBIT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology 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 Anthem's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Anthem was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Network Security

Network security includes the policies and controls in place to manage and monitor the use and security of a computer network and network-accessible resources.

We noted that Anthem has implemented the following network security controls:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A thorough incident response program.

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

1. System Lifecycle Management

Anthem has numerous servers running unsupported versions of operating systems.

A review of Anthem's computer server and database inventories revealed that Anthem has numerous servers running unsupported versions of operating systems. Software vendors typically advertise the dates that they will no longer provide support or distribute security patches for their products (referred to as end-of-life dates). In order to avoid the risk associated with having critical business operations dependent on unsupported software, organizations should have a process in place to anticipate end-of-life dates and phase out the deployment of such software prior to this window of exposure.

We were told that Anthem has an infrastructure lifecycle management program to eliminate end-of-life hardware and operating systems. The goal of the program is to [redacted] However, our review identified [redacted] servers that are running unsupported versions of operating systems and over [redacted] of those have not been supported for more than [redacted]. The large number and significant length time that servers have been unsupported indicates that Anthem's infrastructure lifecycle management program is not effective in its current form.

NIST SP 800-53, Revision 4, recommends that organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer . . . ." NIST SP 800-53, Revision 4, also states that "Unsupported components . . . provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components."

Failure to upgrade system software could leave information systems vulnerable to known attacks without the possibility of remediation.

Recommendation 1

We recommend that Anthem update its policies and procedures to ensure that information systems are upgraded [redacted].

Anthem Response

"Anthem maintains a comprehensive infrastructure lifecycle management program; the program is designed to ensure that server operating systems remain current and supported by vendors. [redacted] ***A 'refresh history' is developed for each server and application within the Anthem environment, detailing the current status of the server or application within the infrastructure lifecycle.***

Anthem tracks the refresh history for each server and application within its environment. As with any business that relies on changing technology, there are certain situations in which migrating applications to a new version would be either impractical or impossible. For example, a mission-critical application may become unstable if migrated to a newer operating system version. In these cases, the Anthem information security team documents the risks associated with maintaining the application and communicates these risks to Anthem business owners as well as IT leadership. Where appropriate, the information security team follows an exceptions process consistent with Anthem's Information Security Risk Exception Request Procedure, provided as Exhibit 1.1. [redacted]

[redacted] ***company acquisitions were migrated into the overall Anthem lifecycle management program, resulting in the integration of*** [redacted] ***new servers into the Anthem environment. Following the acquisitions, Anthem surveyed and prioritized acquired servers for refresh based on the risk profile presented. These systems were integrated into the infrastructure lifecycle management program in*** [redacted]***. A screenshot from Anthem's Security Exception Tracker system, attached as Exhibit 1.2, provides a sample of the documentation created describing risk mitigation efforts for servers that had been acquired by Anthem.***

As part of its ongoing infrastructure lifecycle management program, in the time that has elapsed since the OPM completed its assessment work, [redacted]

[redacted] ***The remaining such servers in the Anthem environment have been integrated into one of the following phases of the refresh process described above:*** [redacted]

OIG Comment

Anthem's response to our draft audit report discusses an "exception process" to document servers that are not refreshed in accordance with the organization's infrastructure lifecycle management program. Although it's beneficial to document the risk associated with maintaining outdated hardware or software, such documentation does little to actually reduce that risk. As mentioned above, [redacted] servers ([redacted] percent of all of Anthem's servers according to the inventory provided during the audit) are unsupported. While we would expect there to be exceptions to a small population of servers, the sheer number of unsupported servers indicates that the infrastructure lifecycle management program is not operating as intended. We continue to recommend that Anthem update its policies and procedures to ensure that information systems are upgraded to current versions prior to the end of vendor support.

2. Server Migration/Integration

Anthem migrated servers into its network that were not fully integrated into its vulnerability management, patching, or configuration management programs.

We performed a credentialed vulnerability assessment using automated tools against a sample of servers selected from Anthem's system inventory. The vulnerability assessment identified numerous servers containing vulnerabilities such as missing patches, noncurrent software, and weak configuration settings. Anthem has relatively mature vulnerability, patch, and configuration management programs in place, so we would have expected the organization to have already detected these vulnerabilities and to have a corrective action plan in place.

Upon further research it was determined that the vast majority of the servers containing vulnerabilities were previously owned and operated by another company that was recently acquired by Anthem. These servers were migrated into Anthem's network, but it is apparent that they were not fully integrated into Anthem's vulnerability management, patching, or configuration management programs.

We believe that Anthem should be extremely cautious when migrating new servers into its technical environment. We acknowledge that Anthem must consider a wide variety of business implications when it acquires new IT assets as part of a merger or acquisition, but the risks associated with introducing vulnerabilities into the environment should be nearly impossible to justify as a business decision. Anthem has dedicated significant time and resources toward implementing IT controls to protect sensitive data, but the introduction of unsecure devices could undermine these efforts.

NIST SP 800-53, Revision 4, states that the organization should scan for "vulnerabilities in the information system and hosted applications [on a routine basis] and when new vulnerabilities potentially affecting the system/applications are identified and reported." NIST SP 800-53, Revision 4, also states that security-relevant software and firmware updates should be installed within timeframes defined by the organization. While Anthem has an adequate process for scanning and patching most of its systems, the process should be applied to all systems.

Recommendation 2

We recommend that Anthem determine what additional controls it can implement to ensure that all servers are fully integrated into the Anthem configuration, patch, and vulnerability management programs before being migrated into the network environment.

Anthem Response

[redacted]

[redacted]

[redacted]

As noted by OPM, the vast majority of the servers containing vulnerabilities were previously owned by other companies that were recently acquired by Anthem. As with all companies that acquire active companies that rely on existing technology to operate their businesses, Anthem must determine how to integrate the acquired company's technology in a manner that is both efficient and sensitive to security concerns.

Anthem is currently reviewing its policies and procedures to further enhance its decision-making framework governing the integration of acquired servers, including by [redacted]

OIG Comment

The evidence received in response to the draft audit report indicates that Anthem's [redacted] *already* required servers to be integrated into Anthem configuration, patch, and vulnerability management programs prior to deployment into the production environment. Anthem also provided evidence that indicates that it has additional policies that require the [redacted]

This additional information increases our concern, as it demonstrates that Anthem violated its own corporate policies by migrating these servers containing security weaknesses into its environment. Therefore, we modified our draft report recommendation and now recommend that Anthem determine what additional controls it can implement to ensure that all servers

are fully integrated into the Anthem configuration, patch, and vulnerability management programs before being migrated into the network environment. Anthem's new requirement to obtain the approval of the [redacted] is a good first step in this process.

Recommendation 3

We recommend that Anthem provide evidence that the vulnerability and configuration issues identified in our assessment specific to the acquired company's servers have been remediated.

Anthem Response

"Anthem will be providing the evidence requested by OPM through established channels. This evidence demonstrates that the vulnerabilities or configuration management issues identified by OPM have been addressed within the Anthem environment. If OPM does not agree that these issues have been remediated, Anthem would appreciate the opportunity to provide additional evidence to OPM prior to publication of OPM's final report."

OIG Comment

As a part of the audit resolution process, we recommend Anthem provide OPM's Healthcare and Insurance Audit Resolution Group with evidence that it has remediated the vulnerability and configuration issues identified in our assessment specific to the acquired company's servers.

B. Configuration Management

Configuration management controls are the policies and procedures that ensure that system software such as operating systems and databases are configured securely. We evaluated Anthem's configuration management program as it relates to the systems that support the processing of FEHBP claims, and determined that the following controls were in place:

Anthem has documented security configuration settings for its operating platforms and performs routine configuration compliance auditing.

- Configuration management policies and procedures;
- Documented baseline configurations for all operating systems in use;
- Routine configuration compliance auditing; and
- A system software change control process.

Although Anthem has a mature configuration management program in place, as mentioned above, these controls have not yet been applied to at least one set of servers that were acquired from another company. We reiterate the importance of enforcing configuration management controls to all devices in Anthem's network.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

INFORMATION SYSTEMS AUDIT GROUP

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Senior Team Leader

[redacted], Group Chief

APPENDIX

BlueCross BlueShield Association

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.626.4800
www.BCBS.com

July 7, 2016

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

Reference: OPM DRAFT IT AUDIT REPORT
Anthem Blue Cross Blue Shield Follow-Up
Audit Report Number 1A-10-62-16-003
(Dated April 27, 2016)

Dear [redacted]:

Please find enclosed a copy of Anthem's responses to the Office of the Inspector General (OIG) recommendations included in the draft audit report of the information technology audit conducted of Anthem, Inc. and dated April 27, 2016. If you have any questions or concerns, please do not hesitate to contact me at [redacted].

Sincerely,

[redacted]
Managing Director
FEP Program Assurance

July 5, 2016

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

Reference: OPM DRAFT IT AUDIT REPORT
Anthem Blue Cross Blue Shield Follow-Up
Audit Report Number 1A-10-62-16-003
(Dated April 27, 2016)

The following represents the Response of Anthem, Inc. to the recommendations included in the draft report of the audit conducted by the Office of the Inspector General at the U.S. Office of Personal Management (OPM). Anthem has appreciated the opportunity to work with OPM's auditors throughout this process.

Anthem's Response contains confidential, proprietary and/or trade secret information of Anthem and/or its affiliated entities and customers. The public use or disclosure of the information provided in this response would cause harm, including competitive harm, to the Company. The information provided Anthem's Response is exempt from public disclosure pursuant to the Freedom of Information Act (FOIA) regulations, 5 U.S.C. § 552. Accordingly, the information provided in this Response, as well as corresponding documentation, may not be released in response to a freedom of information request or under any other circumstances. Should OPM determine that any portion of the information and documentation provided is not exempt from disclosure, Anthem requests that OPM provide two weeks' notice of such determination so that Anthem may take appropriate steps, including obtaining an appropriate protective order or other relief from a court of competent jurisdiction, to protect this information from disclosure. Anthem expressly reserves any applicable privileges or immunities to which it is entitled by applicable law.

Similarly, the current draft of OPM's findings and recommendations also contains confidential, proprietary and/or trade secret information of Anthem and/or its affiliated entities, the public disclosure of which would cause harm, including competitive harm, to Anthem and/or its affiliated entities and customers. For that reason, Anthem will submit a version OPM's draft report that redacts out this highly sensitive information. We repeat the requests in the above paragraph with respect to FOIA and the opportunity to take appropriate steps before any of the redacted information is produced or disclosed. Anthem also requests an opportunity to review the final version of OPM's report, before that document becomes public, in order to review that final report for confidential,

proprietary and/or trade secret information and propose redactions to the final report to protect such information from public disclosure.

We appreciate the opportunity to provide our response to each of the recommendations in this report and request that our comments be incorporated into the Final Audit Report. If you have any questions, please contact me at [redacted].

Sincerely,

[redacted]
Director, FEP Compliance/Internal Control

cc: [redacted]

Anthem's Comments Related to Draft Recommendations

A. Network Security

Plan Response

The network security controls noted by OPM describe a subset of Anthem's comprehensive network security program. Among the information omitted from the description is the fact that Anthem operates a Cyber Security Operations Center ("CSOC"). [redacted]

1. System Lifecycle Management

Recommendation 1

We recommend that Anthem update its policies and procedures to ensure that information systems are upgraded to current versions prior to the end of vendor support.

Anthem Response

Anthem maintains a comprehensive infrastructure lifecycle management program; the program is designed to ensure that server operating systems remain current and supported by vendors. [redacted] A "refresh history" is developed for each server and application within the Anthem environment, detailing the current status of the server or application within the infrastructure lifecycle.

Anthem tracks the refresh history for each server and application within its environment. As with any business that relies on changing technology, there are certain situations in which migrating applications to a new version would be either impractical or impossible. [redacted] In these cases, the Anthem information security team documents the risks associated with maintaining the application and communicates these risks to Anthem business owners as well as IT leadership. Where appropriate, the information security team follows an exceptions process consistent with Anthem's Information Security Risk Exception Request Procedure, provided as Exhibit 1.1. [redacted]

[redacted] company acquisitions were migrated into the overall Anthem lifecycle management program, resulting in the integration of [redacted] new servers into the Anthem environment. Following the acquisitions, Anthem surveyed and prioritized acquired servers for refresh based on the risk profile presented. These systems were integrated into the infrastructure lifecycle management program in [redacted]

[redacted]. A screenshot from Anthem's Security Exception Tracker system, attached as Exhibit 1.2, provides a sample of the documentation created describing risk mitigation efforts for servers that had been acquired by Anthem.

As part of its ongoing infrastructure lifecycle management program, in the time that has elapsed since the OPM completed its assessment work, [redacted] The remaining such servers in the Anthem environment have been integrated into one of the following phases of the refresh process described above: [redacted]

2. Server Migration/Integration

Recommendation 2

We recommend that Anthem update its policies and procedures to require **all** servers to be fully integrated into the Anthem configuration, patch, and vulnerability management program **before** being migrated into the network environment.

Plan Response

[redacted]

As noted by OPM, the vast majority of the servers containing vulnerabilities were previously owned by other companies [redacted]. As with all companies that acquire active companies that rely on existing technology to operate their businesses, Anthem must determine how to integrate the [redacted] technology in a manner that is both efficient and sensitive to security concerns.

Anthem is currently reviewing its policies and procedures to further enhance its decision-making framework governing the integration of acquired servers, including by [redacted]

Recommendation 3

We recommend that Anthem provide evidence that the vulnerability and configuration issues identified in our assessment specific to the acquired company's servers have been remediated.

Plan Response

Anthem will be providing the evidence requested by OPM through established channels. This evidence demonstrates that the vulnerabilities or configuration management issues identified by OPM have been addressed within the Anthem environment. If OPM does not agree that these issues have been remediated, Anthem would appreciate the opportunity to provide additional evidence to OPM prior to publication of OPM's final report.

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