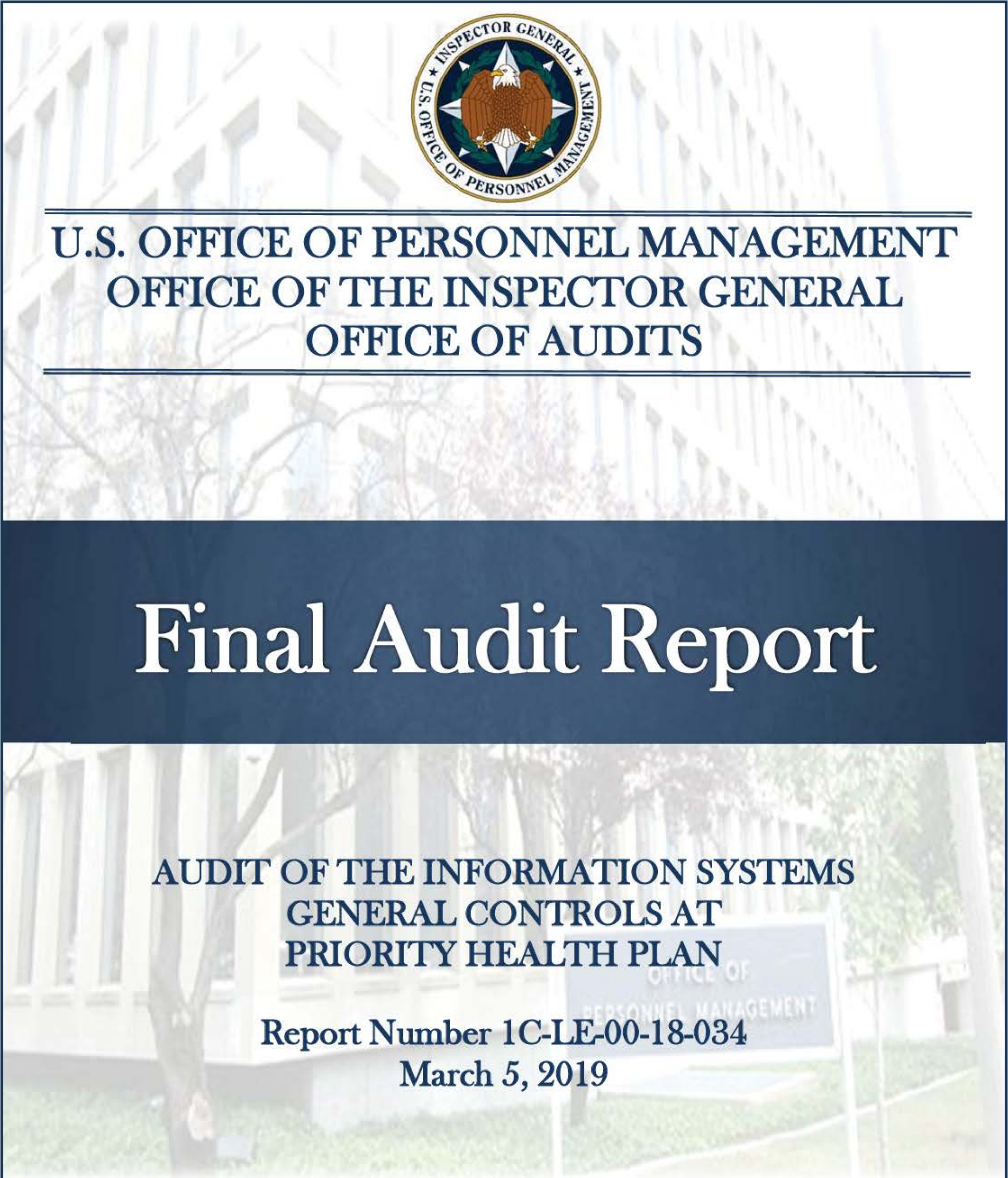


U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT PRIORITY HEALTH PLAN

Report Number 1C-LE-00-18-034
March 5, 2019

EXECUTIVE SUMMARY

Audit of the Information Systems General Controls at Priority Health Plan

Report No. 1C-LE-00-18-034 **March 5, 2019**

Why Did We Conduct The Audit?

Priority Health Plan (Priority Health) is a subsidiary of Spectrum Health System (Spectrum Health) and 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 Priority Health's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by Priority Health to process and store data related to medical encounters and insurance claims for FEHBP members. The audit also included general IT controls managed by Priority Health's parent company, Spectrum Health.

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

Our audit of the IT security controls of Priority Health and Spectrum Health determined that:

- Spectrum Health has implemented an adequate risk assessment methodology.
- Spectrum Health does not routinely review firewall configurations.
- Spectrum Health could improve its network security posture by implementing [redacted] controls.
- Spectrum Health could improve its awareness of system weaknesses by expanding the scope of its vulnerability testing.
- Spectrum Health has adequate policies and procedures to detect and respond to IT security threats.
- Spectrum Health does not have formally documented security configuration standards for its servers. In addition, Spectrum Health is not performing regular reviews of system configurations.
- Spectrum Health's patching process does not currently apply all patch severity levels or third-party application patches.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
COBIT	**Control Objectives for Information and Related Technologies**
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's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
Priority Health	**Priority Health Plan**
Spectrum Health	**Spectrum Health System**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

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

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. SECURITY MANAGEMENT 5

B. NETWORK SECURITY 5
1. Firewall Configuration Review 6
2. [redacted] 6
3. [redacted] 7
4. Vulnerability Scanning 8

C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE 10

D. CONFIGURATION MANAGEMENT 10
1. Security Configuration Standards 11
2. Security Configuration Auditing 12
3. Patch Management 12

APPENDIX: Priority Health Plan's December 7, 2018, response to the draft audit report, issued October 9, 2018.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Priority Health Plan (Priority Health).

The audit was conducted pursuant to FEHBP contract CS 2944; 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.

Priority Health is a subsidiary of Spectrum Health System (Spectrum Health), which offers a wide range of health care products and services in addition to its FEHB line of business. This was our first audit of Priority Health and Spectrum Health's information technology (IT) general security controls. All Priority Health and Spectrum Health 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 Priority Health's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Network security;
- Security Event Monitoring and Incident response; 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 Priority Health'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 Priority Health'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 Priority Health to process medical insurance claims and/or store the data of FEHBP members. Spectrum Health manages many of the information technology resources and processes supporting Priority Health. Therefore, the IT operations of Spectrum Health were considered to be within the scope of this audit. The business processes reviewed are primarily located in Grand Rapids, Michigan.

The onsite portion of this audit was performed in July of 2018. 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 Priority Health as of July, 2018.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Priority Health. 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 Priority Health's business structure and environment;
- Performed a risk assessment of Priority Health'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 to evaluating Priority Health'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;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Control Objectives for Information and Related Technologies (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, Revision 1, An Introduction to Information Security;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;

- 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;

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

- NIST SP 800-123, Guide to General Server Security.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether Priority Health's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Priority Health 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 the examination of the policies and procedures that are the foundation of Priority Health's overall IT security program. We evaluated Priority Health's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Spectrum Health has implemented an adequate IT security management program.

Priority Health's parent company, Spectrum Health, has implemented a series of formal policies and procedures that govern the security management program for Priority Health. Spectrum Health has developed a risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.

Nothing came to our attention to indicate that Spectrum Health does not have an adequate security management program.

B. 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. Spectrum Health manages the technical environment that supports Priority Health's claims adjudication process; we therefore evaluated Spectrum Health's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Adequate remote access controls; and
- Security controls over endpoint devices.

The following sections document several opportunities for improvement related to Priority Health and Spectrum Health's network security controls.

1. **<u>Firewall Configuration Review</u>**

Spectrum Health has implemented firewall devices to control traffic at key locations on its network. Spectrum Health has also documented a firewall standard that details configuration requirements as well as change control procedures for its firewalls. However, there is no policy or procedure requiring routine audits of its firewall configurations.

NIST SP 800-41, Revision 1, states that rulesets should be reviewed or tested periodically to make sure that the firewall rules are in compliance with the organization’s policies.

NIST SP 800-41, Revision 1, also advises that firewall audits can include a detailed examination of all changes to the configuration and may uncover rules that are no longer needed. Failure to routinely audit firewall configurations increases the risk that firewalls are inappropriately configured and may contain rules which allow unacceptable network traffic.

<u>Recommendation 1</u>

We recommend that Spectrum Health/Priority Health update its policies and procedures to include routine audits of its current firewall configurations against its approved firewall policy.

<u>Priority Health Response:</u>

“Priority Health agrees with the recommendation. Priority Health performed a firewall rule audit which included disabling unnecessary and redundant rules. Priority Health is committed to ensuring the firewall configuration is reviewed against approved firewall policy and approvals at least annually.”

<u>OIG Comments:</u>

As part of the audit resolution process, we recommend that Spectrum Health/Priority Health 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 Priority Health agrees to implement.

2. [redacted]

Firewalls are used at [redacted] locations on Spectrum Health’s network [redacted]

[redacted].

NIST SP 800-41, Revision 1, advises that, "Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised by external attackers. Important internal systems should be placed behind internal firewalls." [redacted]

Recommendation 2

[redacted]

Priority Health Response:

"Priority Health agrees with this recommendation. Priority Health has a project to expand [redacted] ***in 2019.*** [redacted]

3. [redacted]

[redacted] However, Spectrum Health had previously identified this weakness and has a project in place to mitigate the issue.

[redacted]

Recommendation 3

We recommend that Spectrum Health/Priority Health implement [redacted].

Priority Health Response:

"Priority Health agrees with this recommendation. Priority Health currently [redacted]

4. Vulnerability Scanning

Vulnerability and Compliance Scan Results

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers in Spectrum Health's network environment. The specific vulnerabilities that we identified were provided to Spectrum Health in the form of an audit inquiry, but will not be detailed in this report.

Spectrum Health could improve its awareness of system weaknesses by expanding the scope of its vulnerability testing.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 4

We recommend that Spectrum Health/Priority Health remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during fieldwork.

Priority Health Response:

"Priority Health agrees with this recommendation. Priority Health has resolved several of the technical weaknesses discovered during the audit and will continue to address outstanding issues as part of its vulnerability management program in 2019."

Scan Configuration

Our scan results identified several vulnerabilities with significant severity levels according to the Common Vulnerability Scoring System. We asked Spectrum Health personnel if they had previously detected these vulnerabilities and they responded that they were unaware due to the configuration of their scanning tool, which is only configured to detect vulnerabilities above a certain severity level. However, Spectrum Health's policies require the vulnerabilities with the severity we found in our scans to be remediated within defined timeframes.

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 ... ." Failure to properly configure its scan tool increases the risk that undetected vulnerabilities can be compromised by attackers.

Recommendation 5

We recommend that Spectrum Health/Priority Health implement procedures to scan for all significant vulnerability severity levels to ensure patching is completed according to its policy.

Priority Health Response:

"Priority Health agrees with this recommendation. Security vulnerability scanning policies, standards, and procedures are being actively updated to better align with HIPAA and NIST guidance to address the gaps between operational process and policy statements. This work is targeted for completion in 2019."

Scan Scope

Our vulnerability testing included a wide range of server types and operating systems. As noted above, our scan exercise found vulnerabilities on several of these systems. Spectrum Health personnel stated that they were unaware of some of the vulnerabilities because they only conduct scans on a subset of the network. However, Spectrum Health has a policy in place stating that its production systems shall support weekly vulnerability scanning. Spectrum Health communicated that it intends to expand the scope of the scans in the future.

NIST SP 800-123 states that "Periodic security testing of servers is critical. Without periodic testing, there is no assurance that current protective measures are working or that the security patch applied by the server administrator is functioning as advertised." Failure to perform full scope vulnerability scans increases the risk that Spectrum Health information systems could be compromised and sensitive data stolen or destroyed.

<u>Recommendation 6</u>

We recommend that Spectrum Health/Priority Health update its policies to ensure credentialed scans are routinely conducted on its entire network environment.

<u>Priority Health Response:</u>

"Priority Health agrees with this recommendation. Priority Health Cyber Threat Management Team already performs credentialed scans and is actively updating its processes to ensure credentialed scans occur through compliance monitoring where possible."

C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Spectrum Health has adequate policies and procedures to detect and respond to IT security threats.

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. Spectrum Health manages the technical environment that supports Priority Health's claims adjudication process; we therefore evaluated Spectrum Health's processes related to monitoring and responding to security and privacy events.

Our review found the following controls in place:

- Security event monitoring throughout the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

Nothing came to our attention to indicate that Spectrum Health does not have an adequate security event monitoring or incident response program.

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. Spectrum Health employs a team of technical personnel who manage system software configuration for the organization. We evaluated Spectrum Health's management of the configuration of its computer servers and databases.

Our review found the following controls in place:

- Documented security configuration management policy;

- Documented system change control process; and

- Effective policies and procedures to ensure that unsupported system software is not in use.

The sections below document areas for improvement related to Spectrum Health's configuration management controls.

1. <u>Security Configuration Standards</u>

Spectrum Health has a standardized process to deploy new servers from pre-established templates. Security policies are then applied to certain systems according to functional or regulatory requirements. However, Spectrum Health does not have common security configuration standards that are enforced on all systems within its environment. Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements … ."

In addition, NIST SP 800-53, Revision 4, states that an organization must develop, document, and maintain a current baseline configuration of the information system. Failure to establish approved system configuration settings increases the risk that the system may not be configured in a secure manner.

Recommendation 7

We recommend that Spectrum Health/Priority Health document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

Priority Health Response:

"Priority Health agrees with this recommendation. Priority Health has an active initiative to enhance baseline security configurations for deployed operating system platforms and databases. This work is targeted for completion in 2019."

2. Security Configuration Auditing

As noted above, Spectrum Health does not maintain approved security configuration standards for its operating platforms, and therefore cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system. Failure to implement a configuration compliance auditing program increases the risk that servers are not configured appropriately and left undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 8

We recommend that Spectrum Health/Priority Health implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

Priority Health Response:

"Priority Health agrees with this recommendation. Subsequent to completion of item (7), Priority Health will monitor and periodically audit systems to ensure compliance with approved security configurations. This work is targeted for completion in 2019."

3. Patch Management

Spectrum Health uses several tools to centrally manage the installation of security patches across its information systems and has a security configuration policy that establishes a requirement for prioritizing and deploying patches according to a defined schedule.

As a result of our vulnerability testing, we identified several instances of software that was missing patches or in some cases was running unsupported versions. Spectrum Health informed us that some of these missing patches were due to limitations of the organization's patching tools. They also stated that for some applications, the organization relies on the end-user to keep the software up to date. These issues are compounded by the fact that Spectrum Health does not perform vulnerability scanning on all systems, which could help identify patches missing from these systems.

NIST SP 800-53, Revision 4, states that the organization should identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly. Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

Recommendation 9

We recommend that Spectrum Health/Priority Health update its patching procedures to ensure that production servers are updated with all appropriate patches, service packs, and hotfixes.

Priority Health Response:

"Priority Health agrees with this recommendation. Priority Health has an initiative to further improve our patching procedures for all servers. This will include additional oversight to ensure appropriate patching levels are applied. This work is targeted for completion in 2019."

Recommendation 10

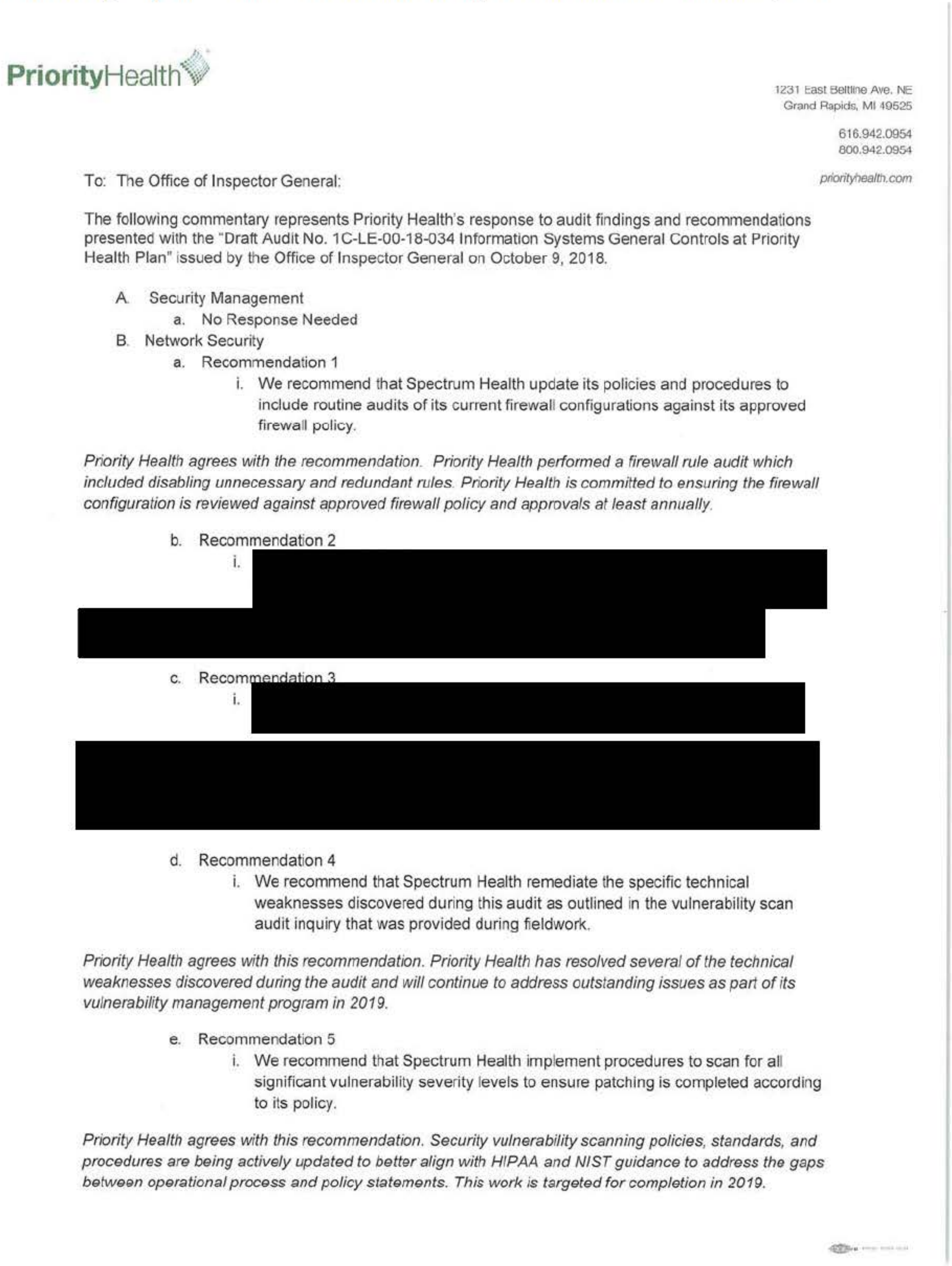
We recommend that Spectrum Health/Priority Health assess its management of third-party software patching and implement controls to ensure that appropriate updates are installed on a timely basis.

Priority Health Response:

"Priority Health agrees with this recommendation. Priority Health has an initiative to expand the scope of its current scanning program to include additional credentialed scans of key systems. This work is targeted for completion in 2019."

APPENDIX

The following response was received from Priority Health Plan on December 7, 2018.



PriorityHealth

1231 East Beltline Ave. NE
Grand Rapids, MI 49525

616.942.0954
800.942.0954

priorityhealth.com

To: The Office of Inspector General:

The following commentary represents Priority Health's response to audit findings and recommendations presented with the "Draft Audit No. 1C-LE-00-18-034 Information Systems General Controls at Priority Health Plan" issued by the Office of Inspector General on October 9, 2018.

A. Security Management
   a. No Response Needed
B. Network Security
   a. Recommendation 1
      i. We recommend that Spectrum Health update its policies and procedures to include routine audits of its current firewall configurations against its approved firewall policy.

Priority Health agrees with the recommendation. Priority Health performed a firewall rule audit which included disabling unnecessary and redundant rules. Priority Health is committed to ensuring the firewall configuration is reviewed against approved firewall policy and approvals at least annually.

   b. Recommendation 2
      i. [redacted]

   c. Recommendation 3
      i. [redacted]

   d. Recommendation 4
      i. We recommend that Spectrum Health remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during fieldwork.

Priority Health agrees with this recommendation. Priority Health has resolved several of the technical weaknesses discovered during the audit and will continue to address outstanding issues as part of its vulnerability management program in 2019.

   e. Recommendation 5
      i. We recommend that Spectrum Health implement procedures to scan for all significant vulnerability severity levels to ensure patching is completed according to its policy.

Priority Health agrees with this recommendation. Security vulnerability scanning policies, standards, and procedures are being actively updated to better align with HIPAA and NIST guidance to address the gaps between operational process and policy statements. This work is targeted for completion in 2019.

f. Recommendation 6

   i. We recommend that Spectrum Health update its policies to ensure credentialed scans are routinely conducted on its entire network environment.

Priority Health agrees with this recommendation. Priority Health Cyber Threat Management Team already performs credentialed scans and is actively updating its processes to ensure credentialed scans occur through compliance monitoring where possible.

C. Security Event Monitoring and Incident Repose

   a. No Response Needed

D. Configuration Management

   a. Recommendation 7

      i. We recommend that Spectrum Health document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

Priority Health agrees with this recommendation. Priority Health has an active initiative to enhance baseline security configurations for deployed operating system platforms and databases. This work is targeted for completion in 2019.

   b. Recommendation 8

      i. We recommend that Spectrum Health implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards

Priority Health agrees with this recommendation. Subsequent to completion of item (7), Priority Health will monitor and periodically audit systems to ensure compliance with approved security configurations. This work is targeted for completion in 2019.

   c. Recommendation 9

      i. We recommend that Spectrum Health update its patching procedures to ensure that production servers are updated with all appropriate patches, service packs, and hotfixes

Priority Health agrees with this recommendation. Priority Health has an initiative to further improve our patching procedures for all servers. This will include additional oversight to ensure appropriate patching levels are applied. This work is targeted for completion in 2019.

   d. Recommendation 10

      i. We recommend that Spectrum Health assess its management of third-party software patching and implement controls to ensure that appropriate updates are installed on a timely basis.

Priority Health agrees with this recommendation. Priority Health has an initiative to expand the scope of its current scanning program to include additional credentialed scans of key systems. This work is targeted for completion in 2019.

Sincerely,

John Carl
Director - Information Services
Priority Health Applications

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