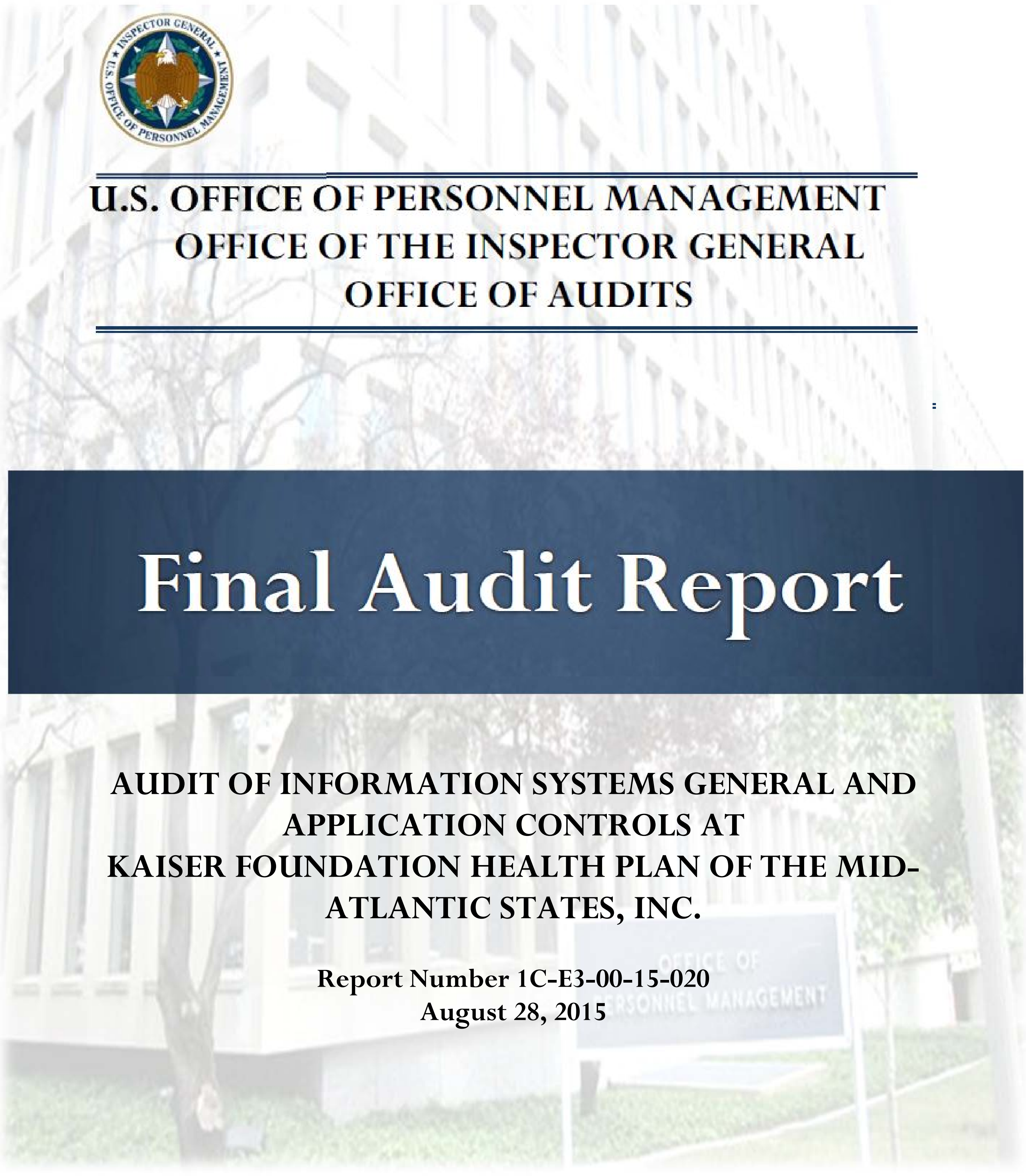

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT KAISER FOUNDATION HEALTH PLAN OF THE MID-ATLANTIC STATES, INC.

Report Number 1C-E3-00-15-020
August 28, 2015

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc.

Report No 1C-E3-00-15-020 **August 28, 2015**

Background

Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. (Kaiser) 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 Kaiser's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by Kaiser 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 Kaiser determined that:

- Kaiser has established an adequate security management program.
- Kaiser has implemented a variety of controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, we noted several areas of concern related to Kaiser's access controls:
  - Physical access controls over Kaiser's data center could be improved.
  - The current process of revoking physical access privileges of terminated employees could be improved.
  - Kaiser does not require [redacted] for privileged user system access.
- Kaiser has implemented an incident response and network security program. However, we noted several areas of concern related to Kaiser's network security controls:
  - A patch management policy is in place, but our test work indicated that patches are not being implemented in a timely manner.
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized.
- Kaiser has developed formal configuration management policies and has approved baseline configurations for its operating platforms. However, our test work indicated that several servers contained insecure configurations.
- Kaiser's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. Kaiser 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.
- Kaiser has implemented multiple controls over its member encounters and claims adjudication processes to ensure that FEHBP encounters and claims are processed accurately.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information Systems Control Audit Manual**
GAO	**U.S. Government Accountability Office**
HIO	**Healthcare and Insurance Office**
IT	**Information Technology**
Kaiser	**Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc.**
NIST	**National Institute of Standards and 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	**Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc.**

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 Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. (Kaiser or Plan).

The audit was conducted pursuant to FEHBP contract CS 1763; 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.

This was our first audit of Kaiser's information technology (IT) general and application controls.

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 Kaiser's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation of duties;
- Contingency planning; and
- Application controls specific to Kaiser's member encounters process.

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 Kaiser'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 Kaiser'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 Kaiser to process and/or store the data of FEHBP members. The business processes reviewed are primarily located in [redacted], Maryland.

The on-site portion of this audit was performed in January and February, 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 and application controls in place at Kaiser as of March 2015.

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

- Gathered documentation and conducted interviews;
- Reviewed Kaiser's business structure and environment;
- Performed a risk assessment of Kaiser'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 Kaiser'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 800-30 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, Computer Security Incident Handling Guide.

Compliance with Laws and Regulations

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

Kaiser maintains a series of thorough IT security policies and procedures.

Kaiser has implemented a series of formal policies and procedures that comprise its security management program. Kaiser has developed an adequate risk management methodology, and has procedures to document, track, and mitigate or accept identified risk. We also reviewed Kaiser's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Kaiser 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 Kaiser's facilities and data centers. We also examined the logical controls protecting sensitive data on Kaiser's network environment and claims processing related applications.

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

- Procedures for granting, adjusting, and auditing user access;
- Procedures for removing network and application access for terminated employees; and
- Policies and procedures for granting and revoking physical access to the data center.

However, the following section documents several opportunities for improvement related to Kaiser's access controls.

1. Authentication Standards

We identified information systems that are not configured to enforce password [redacted] [redacted] restrictions. Kaiser's User Access Management policy only requires passwords to be [redacted] for computing systems/devices that do not require and enforce [redacted]

[redacted]. However, requiring all passwords to be [redacted] is a control that we observe at other FEBHP carriers and is considered an industry best practice.

NIST SP 800-53 Revision 4 states that organizations should configure information systems to enforce password [redacted] restrictions. FISCAM also states that passwords protecting sensitive data and functions should be [redacted].

Failure to require [redacted] increases the risk that a user account could be compromised and allow [redacted] unauthorized access to sensitive and proprietary information.

__Recommendation 1__
We recommend that Kaiser configure all of its information systems to enforce [redacted] password [redacted].

__Plan Response:__
"The Carrier recognizes the importance of the recommendation. The Carrier's current password policy (SS.112.PW.004.01) does not require a standard password [redacted] [redacted], as [redacted] in some systems represent risks to patient safety. Therefore, password [redacted] is not enforced globally, but is utilized as a control at the application level where it is an appropriate approach. For systems where [redacted] is a viable approach, such as PCI, [redacted] are enforced through a targeted policy. The Carrier also imposes standards for minimum password [redacted]. In addition, to further reduce risk, on a periodic basis the Carrier performs user access reviews to ensure that access is appropriate.

The Carrier is evaluating and will implement changes to password policies and practices as appropriate. This review will be based on relevant factors, including operational requirements and the sensitivity of information."

__OIG Reply:__
As part of the audit resolution process, we recommend that Kaiser provide OPM's Healthcare and Insurance Office with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this report that Kaiser agrees to implement.

2. Privileged User Authentication

Privileged users (system administrators) of Kaiser's information systems use temporary privilege elevation methods or a secondary administrator account when elevated privileges are needed. While these are good controls, Kaiser's management of privileged user accounts could be improved with the use of [redacted].

OMB Memorandum [redacted] requires the use of [redacted] to access all federal information systems. We expect all FEHBP contractors to use [redacted] for, at a minimum, administrator-level access to information systems. Failure to use [redacted] increases the risk that privileged user accounts could be compromised, thereby allowing unauthorized individuals access to sensitive and proprietary information.

<u>Recommendation 2</u>

We recommend that Kaiser implement [redacted] for privileged user access to all information systems.

<u>Plan Response:</u>

"The Carrier agrees that [redacted] is an important control for privileged user access. We are currently in the process of removing privileged accounts from the host layer and moving to a [redacted] model that uses [redacted] when requesting a temporary account. Accounts are active for a maximum of [redacted], and the password is changed upon [redacted]. The Carrier has started deploying this model to select environments, and will be expanding to other server types this year. The Carrier also is investigating [redacted] in other settings, and anticipates taking a risk based approach to deployment."

3. Physical Access Removal

Kaiser's process for removing physical access privileges could be improved.

We compared a list of employees with active access to Kaiser facilities in the Mid-Atlantic region to a list of employees that were terminated in the prior year. We identified over 50 terminated employees whose physical access cards remained active. We also identified more than 150 duplicate access badges that remained active after replacement badges were issued. None of the employees that retained access following termination had access to the data center. Kaiser deactivated the problematic access cards during the fieldwork phase of our audit, but will need to implement controls to ensure that the issue does not reoccur in the future. Kaiser does not currently have a process in place to routinely audit employees' physical access to non-datacenter facilities.

NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," states that an organization must terminate access upon termination of employment. NIST SP 800-53 Revision 4 also states that an organization must review and analyze system audit records for indications of inappropriate or unusual activity. Failure to remove and audit physical access to terminated users increases the risk that a terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information.

Recommendation 3
We recommend that Kaiser implement a methodology to ensure that physical access to facilities is removed promptly when access is no longer required.

Plan Response:
"The Carrier has implemented an improved series of protocols to ensure only individuals that are actively working for the Carrier have badge access. These include two channels of termination and retirement reporting to the Regional Security Department, followed by appropriate review, research and documentation of security actions. This improved process was fully implemented June 1, 2015."

Recommendation 4
We recommend that Kaiser implement a methodology to discover unauthorized or duplicate access accounts.

Plan Response:
"The improved process described in response to Recommendation 3 above will support prompt discovery and remediation of unauthorized access and duplicate accounts. Please note, however, that several members of the Mid-Atlantic Security Team require multiple badges to ensure that they have after-hours and emergency incident response access to Kaiser's facilities. Other staff will have existing badges de-activated when an access card is added or modified."

4. Data Center Physical Access Controls

Kaiser's data center uses electronic card readers to control physical access. While the data center has several physical access controls including real-time video monitoring and a man-trap in the lobby, we expect all FEHBP contractors to also have [redacted] at data center entrances. Kaiser should implement the access controls listed below that we typically see at other FEHBP carrier facilities.

- [redacted]; and
- [redacted]

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to Kaiser's data centers and the sensitive IT resources and confidential data they contain. NIST SP 800-53 Revision 4 provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 5

We recommend that Kaiser reassess its data centers' physical access management and implement controls that will ensure proper physical security. At a minimum, Kaiser should implement [redacted] [redacted] [redacted] at data center entrances.

Plan Response:

"The Carrier's management approved implementing the recommendation for [redacted] at the production national data centers including the Maryland data center. A pilot of the proposed technologies was held during the week of May 21, 2015. Based on pilot results, a plan has been developed for implementation of [redacted] as well as [redacted] at the production national data centers including the Maryland data center by the end of 2015."

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 Kaiser's network security program and also independently performed several automated vulnerability scans and configuration compliance audits on Kaiser's systems during this audit. The detailed findings of our automated scans were provided to Kaiser during the audit, but due to their sensitive nature, will only be referenced at a high level in this report. We noted the following opportunities for improvement related to network security controls.

1. Vulnerabilities Identified in Scans

System Patching

Kaiser has documented vulnerability management policies and procedures that establish timeframes for remediating weaknesses. Kaiser also conducts routine vulnerability scanning on its entire technical environment. However, the results of our vulnerability scans indicate that all critical patches, service packs, and hot fixes are not implemented in a timely manner.

FISCAM states that "software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 4 states that the Plan must 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.

Recommendation 6

We recommend that Kaiser implement procedures and controls to ensure that production servers are updated with appropriate patches, service packs, and hotfixes on a timely basis.

Plan Response:

"In response to Recommendations 6 and 7, the Carrier is reviewing its Enterprise Patch and Vulnerability Management Program to ensure that production servers are updated with appropriate patches, service packs, and hot-fixes on a timely basis. The Carrier also is establishing Enterprise Patch and Vulnerability Governance to provide oversight for ensuring software is scanned and updated frequently to guard against known vulnerabilities and to identify, report, and correct information system flaws and install security-relevant software updates promptly.

Where system changes are required to address vulnerabilities discovered by the OIG scan, most remediation is expected to be complete by August 2015. We are furthermore reviewing our overall vulnerability management program and making enhancements for the broader environment."

Noncurrent software

The results of the vulnerability scans also indicated that several servers contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 7

We recommend that Kaiser implement a process to ensure that only current and supported versions of software applications are installed on the production servers.

Plan Response:

"Please see the response to Recommendation number 6 above."

D. Configuration Management

We evaluated Kaiser's process for managing the configuration of the operating systems and databases that process federal data and determined that the following controls were in place:

- Documented configuration baselines;
- Routine configuration compliance scanning; and
- Thorough change management procedures for system software and hardware.

However, the results of our vulnerability scans indicated that several servers contained insecure configurations that could allow hackers or unprivileged users to gain unauthorized access to sensitive and proprietary information.

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

Recommendation 8

We recommend that Kaiser remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Plan Response:

"The Carrier is actively remediating configuration settings discovered as vulnerable by audit vulnerability scans, to ensure systems comply with the Carrier's documented configuration baseline. The Carrier's configuration baseline is based on industry accepted standards and is updated with an [redacted]. The majority of remediation will be completed by August 2015."

E. Contingency Planning

Kaiser has adequate controls over its contingency planning process.

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

- Disaster recovery plan;
- Business continuity plan;
- Disaster recovery plan tests; and
- Emergency response procedures.

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems." Kaiser 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 Kaiser has not implemented adequate controls related to contingency planning.

F. Application Controls

The following sections detail our review of the controls specific to the applications supporting Kaiser's processing of medical encounters and insurance claims for FEHBP members.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of applications that process and/or store federal data.

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

- Kaiser has implemented practices that allow modification to be tracked throughout the change process;
- Unit, system, and user acceptance testing are all conducted in accordance with a documented testing strategy; and
- Kaiser uses a business unit independent from the software developers to move the code between development and production environments to ensure adequate segregation of duties.

Nothing came to our attention to indicate that Kaiser has not implemented adequate controls related to the application configuration management process.

2. Member Encounters and Claims Processing

We evaluated the input, processing, and output controls associated with Kaiser's electronic transactions related to member encounters and claims adjudication. We determined that Kaiser has implemented policies and procedures to help ensure:

- Sufficient input, processing, and output controls over the member encounters and claims adjudication process;
- Encounters and claims are monitored as they are processed through the systems 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 Kaiser has not implemented adequate controls related to member encounters or claims processing.

3. **Enrollment**
We evaluated Kaiser's procedures for managing its database of member enrollment data. Enrollment information is received electronically or in paper format and entered into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately. We do not have any concerns regarding Kaiser's enrollment policies and procedures.

4. **Debarment**
Kaiser has adequate procedures for reviewing its employee and provider files for debarments and suspensions. Kaiser downloads the OPM OIG debarment list monthly and imports the list into a tool that automatically compares the entries to Kaiser's employee and provider files; any potential matches are reviewed and confirmed. Debarred providers are then terminated in the system.

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

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

Appendix

KAISER PERMANENTE®

June 15, 2015

Via Email ([redacted]@opm.gov)

[redacted]
Auditor-in-Charge
Information Systems Audit Group
U.S. Office of Personnel Management
Office of the Inspector General
1900 E Street N.W., Room 6400
Washington, D.C. 20415

Re: Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. (Contract CS 1763) - Response to Draft of a Proposed Report 1C-E3-00-15-020 (April 14, 2015)

Dear [redacted]:

This letter responds to your correspondence of April 14, 2015, which enclosed a Draft of a Proposed Report (Draft Report) based on "... the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. (Kaiser)." Draft Report, p. 1. This response addresses recommendations in the Draft Report. Where appropriate, it also outlines corrective actions that have been taken or will be taken by Kaiser based on the recommendations.

As you requested, we are submitting copies of this document electronically.

I. SUMMARY OF DRAFT REPORT RECOMMENDATIONS

As described in the Draft Report, OIG identified several opportunities for improvement and made eight (8) recommendations with regard to the information systems subject to audit. In brief, the Draft Report made the following recommendations:

1) Configure all information systems to enforce routine password changes in accordance with the corporate policy
2) Implement [redacted] for privileged user access to all information systems
3) Implement a methodology to ensure that physical access to facilities is removed promptly when access is no longer required
4) Implement a methodology to discover unauthorized or duplicate access accounts

5) Reassess data center physical access management and implement controls that will ensure proper physical security. At a minimum, Kaiser should implement [redacted] [redacted] [redacted] at data center entrances
6) Implement procedures and controls to ensure that production servers are updated with appropriate patches, service packs, and hotfixes on a timely basis
7) Implement a process to ensure that only current and supported versions of software applications are installed on the production servers
8) Remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit

II. RESPONSE TO DRAFT REPORT FINDINGS

Kaiser generally applauds the many positive observations and findings in the Draft Report, and views these as affirmation of the significant expenditures of time, effort and resources that Kaiser has undertaken to develop, build, and secure its information technology environment. In several instances, the Draft Report has helped Kaiser identify opportunities to improve the programs, processes, systems and plans it already has in place.

In addition however, Kaiser wishes to reiterate or identify additional facts which we believe clarify or place in context a number of the findings in the Draft Report. With regard to many of the opportunities for improvement identified in the Draft Report, Kaiser already has addressed or is in the process of implementing plans to address these opportunities and has provided additional details in the discussion below. Continued development and implementation of these programs may depend on budgetary constraints. We would be pleased to provide any additional information that would help satisfy concerns noted in the Draft Report.

Recommendation 1 (B. Access Controls; 1. Authentication Standards):

Kaiser policy states that users are required to [redacted] *their passwords* [redacted] [redacted]*. However, we identified information systems that are not configured to enforce this policy. NIST SP 800-53 Revision 4 states that organizations should configure information systems to enforce password* [redacted] *restrictions. FISCAM also states that passwords protecting sensitive data and functions should be* [redacted]*.*

Failure to require [redacted] *increases the risk that a user account could be compromised and allow* [redacted] *unauthorized access to sensitive and proprietary information.*

Recommendation 1

We recommend that Kaiser configure all of its information systems to enforce [redacted] password [redacted] in accordance with the corporate policy.

Carrier Response:

The Carrier recognizes the importance of the recommendation. The Carrier's current password policy (SS.112.PW.004.01) does not require a standard password [redacted], as [redacted] in some systems represent risks to patient safety. Therefore, password [redacted] is not enforced globally, but is utilized as a control at the application level where it is an appropriate approach. For systems where [redacted] is a viable approach, such as PCI, [redacted] are enforced through a targeted policy. The Carrier also imposes standards for minimum password [redacted]. In addition, to further reduce risk, on a periodic basis the Carrier performs user access reviews to ensure that access is appropriate.

The Carrier is evaluating and will implement changes to password policies and practices as appropriate. This review will be based on relevant factors, including operational requirements and the sensitivity of information.

<u>Recommendation 2 (B. Access Controls; 2. Privileged User Authentication)</u>:

Privileged users (system administrators) of Kaiser's information systems use temporary privilege elevation methods or a secondary administrator account when elevated privileges are needed. While these are good controls, Kaiser's management of privileged user accounts could be improved with the use of [redacted].

OMB Memorandum [redacted] requires the use of [redacted] to access all federal information systems. We expect all FEHBP contractors to use [redacted] for, at a minimum, administrator-level access to information systems. Failure to use [redacted] increases the risk that privileged user accounts could be compromised, thereby allowing unauthorized individuals access to sensitive and proprietary information.

Recommendation 2

We recommend that Kaiser implement [redacted] for privileged user access to all information systems.

Carrier Response:

The Carrier agrees that [redacted] is an important control for privileged user access. We are currently in the process of removing privileged accounts from the host layer and moving to a [redacted] model that uses [redacted] when requesting a temporary account. Accounts are active for a maximum of [redacted], and the password is changed upon [redacted]. The Carrier has started deploying this model to select environments, and will be expanding to other server types this year. The Carrier also is investigating [redacted] in other settings, and anticipates taking a risk based approach to deployment.

Recommendations 3 & 4 (B. Access Controls; 3. Physical Access Removal):

We compared a list of employees with active access to Kaiser facilities in the Mid-Atlantic region to a list of employees that were terminated in the prior year. We identified over 50 terminated employees whose physical access cards remained active. We also identified more than 150 duplicate access badges that remained active after replacement badges were issued. None of the employees that retained access following termination had access to the data center. Kaiser deactivated the problematic access cards during the fieldwork phase of our audit, but will need to implement controls to ensure that the issue does not reoccur in the future. Kaiser does not currently have a process in place to routinely audit employees' physical access to non-datacenter facilities.

NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," states that an organization must terminate access upon termination of employment. NIST SP 800-53 Revision 4 also states that an organization must review and analyze system audit records for indications of inappropriate or unusual activity. Failure to remove and audit physical access to terminated users increases the risk that a terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information.

Recommendation 3
We recommend that Kaiser implement a methodology to ensure that physical access to facilities is removed promptly when access is no longer required.

Carrier Response:
The Carrier has implemented an improved series of protocols to ensure only individuals that are actively working for the Carrier have badge access. These include two channels of termination and retirement reporting to the Regional Security Department, followed by appropriate review, research and documentation of security actions. This improved process was fully implemented June 1, 2015.

Recommendation 4
We recommend that Kaiser implement a methodology to discover unauthorized or duplicate access accounts.

Carrier Response:
The improved process described in response to Recommendation 3 above will support prompt discovery and remediation of unauthorized access and duplicate accounts. Please note, however, that several members of the Mid-Atlantic Security Team require multiple badges to ensure that they have after-hours and emergency incident response access to Kaiser's facilities. Other staff will have existing badges de-activated when an access card is added or modified.

Recommendation 5 (B. Access Controls; 4. Data Center Physical Access):

Kaiser's data center uses electronic card readers to control physical access. While the data center has several physical access controls including real-time video monitoring and a man-trap in the lobby, we expect all FEHBP contractors to also have [redacted] at data center entrances. Kaiser should implement the common access controls listed below that we typically see at other FEHBP carrier facilities.

- [redacted] *and*
- [redacted]

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to Kaiser's data centers and the sensitive IT resources and confidential data they contain. NIST SP 800-53 Revision 4 provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 5
We recommend that Kaiser reassess its data centers' physical access management and implement controls that will ensure proper physical security. At a minimum, Kaiser should implement [redacted] [redacted] [redacted] *at data center entrances.*

Carrier Response:
The Carrier's management approved implementing the recommendation for [redacted] as well as [redacted] at the production national data centers including the Maryland data center. A pilot of the proposed technologies was held during the week of May 21, 2015. Based on pilot results, a plan has been developed for implementation of [redacted] as well as [redacted] at the production national data centers including the Maryland data center by the end of 2015.

Recommendation 6 (C. Network Security; 1. Vulnerabilities Identified in Scans – *System Patching*):

Kaiser has documented vulnerability management policies and procedures that establish timeframes for remediating weaknesses. Kaiser also conducts routine vulnerability scanning on its entire technical environment. However, the results of our vulnerability scans indicate that all critical patches, service packs, and hot fixes are not implemented in a timely manner.

FISCAM states that "software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 4 states that the Plan must 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.

Recommendation 6
We recommend that Kaiser implement procedures and controls to ensure that production servers are updated with appropriate patches, service packs, and hotfixes on a timely basis.

Carrier Response:
In response to Recommendations 6 and 7, the Carrier is reviewing its Enterprise Patch and Vulnerability Management Program to ensure that production servers are updated with appropriate patches, service packs, and hot-fixes on a timely basis. The Carrier also is establishing Enterprise Patch and Vulnerability Governance to provide oversight for ensuring software is scanned and updated frequently to guard against known vulnerabilities and to identify, report, and correct information system flaws and install security-relevant software updates promptly.

Where system changes are required to address vulnerabilities discovered by the OIG scan, most remediation is expected to be complete by August 2015. We are furthermore reviewing our overall vulnerability management program and making enhancements for the broader environment.

Recommendation 7 (C. Network Security; 1. Vulnerabilities Identified in Scans – *Noncurrent Software*):

The results of the vulnerability scans also indicated that several servers contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 7
We recommend that Kaiser implement a process to ensure that only current and supported versions of software applications are installed on the production servers.

Carrier Response:
Please see the response to Recommendation number 6 above.

Recommendation 8 (D. Configuration Management):

We evaluated Kaiser's configuration management of the operating systems and databases supporting member encounters and claims processing and determined that the following controls were in place:

- *Documented configuration baselines;*
- *Routine configuration compliance scanning; and*
- *Thorough change management procedures for system software and hardware.*

However, the results of our vulnerability scans indicated that several servers contained insecure configurations that could allow hackers or unprivileged users to gain unauthorized access to sensitive and proprietary information.

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

Recommendation 8
We recommend that Kaiser remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Carrier Response:
The Carrier is actively remediating configuration settings discovered as vulnerable by audit vulnerability scans, to ensure systems comply with the Carrier's documented configuration baseline. The Carrier's configuration baseline is based on industry accepted standards and is updated with an [redacted]. The majority of remediation will be completed by August 2015.

III. CONCLUSION

We appreciate this opportunity to respond to the Draft Report, and urge OPM to give due consideration to the information provided in this letter.

This response contains commercial and financial information that is proprietary and confidential to the Carrier. Disclosure of this information would cause substantial harm to the Carrier's competitive position. OPM is requested to treat this document as confidential. This material is exempt from disclosure under Section 552(b)(4) of Title 5 of the United States Code.

Please do not hesitate to contact me if you have any questions or need any additional information. You can reach me at [redacted]. Thank you.

Sincerely,

/s/ [redacted]

[redacted]
Vice President, FEHBP Line of Business

cc: [redacted]

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