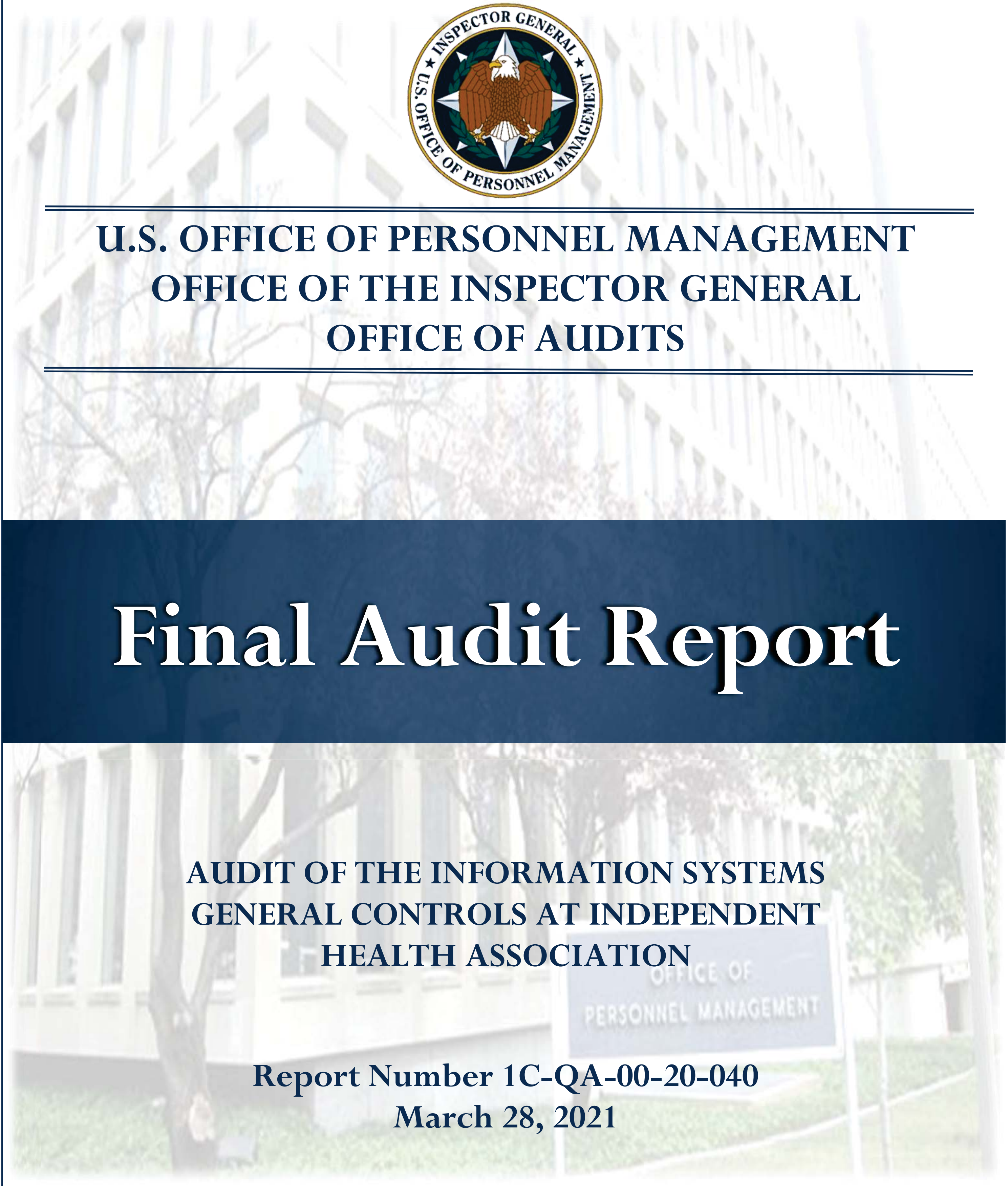
U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS



Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT INDEPENDENT HEALTH ASSOCIATION

Report Number 1C-QA-00-20-040
March 28, 2021

EXECUTIVE SUMMARY

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT INDEPENDENT HEALTH ASSOCIATION

Report No. 1C-QA-00-20-040 **March 28, 2021**

Why Did We Conduct The Audit?

Independent Health Association (IH) 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 IH's information technology (IT) environment.

What Did We Audit?

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

- IH has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified during risk assessments. IH also performs risk assessments of its third party vendors.
- IH has firewalls at the edge of its network to control traffic from external connections and vendors.
- IH monitors database and user activity; however, it does not currently monitor wireless network activity.
- IH has an established incident response program.
- IH has documented and implemented a system configuration change control process.
- IH has developed security configuration standards for some of the operating systems in its environment. However, standards for all of its operating systems have not been established. IH also does not perform routine reviews of its security configurations.
- [redacted] IH [redacted] has not developed system software lifecycle policies or procedures to ensure that software is upgraded or removed prior to the end of vendor support.

ABBREVIATIONS

CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information System Controls Audit Manual
GAO	U.S. Government Accountability Office
IH	Independent Health Association
IT	Information Technology
NIST SP	National Institute of Standards and Technology’s Special Publication
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

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

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 4

A. SECURITY MANAGEMENT 4

B. NETWORK SECURITY 4

C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE 5

1. Wireless Event Monitoring 5

D. CONFIGURATION MANAGEMENT 6

1. Security Configuration Standards 6
2. Security Configuration Auditing 7
3. System Lifecycle Management 8

APPENDIX: Independent Health Association's February 2, 2021, response to the draft audit report, issued December 10, 2020.

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 Independent Health Association (IH).

The audit was conducted pursuant to FEHBP contract CS 1933; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act, enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for Federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our first audit of the information technology (IT) general security controls at IH. All IH personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in IH's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Network security;
- 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 IH'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 IH'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 IH to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Buffalo, New York.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general controls in place over IH's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at IH as of March 2021.

In conducting our audit, we relied to varying degrees on computer-generated data provided by IH. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this audit, we:

- Performed a risk assessment of IH's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM);

- Gathered documentation and conducted interviews;

- Reviewed IH's business structure and environment; and

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

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

- GAO's FISCAM; and

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

COMPLIANCE WITH LAWS AND REGULATIONS

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

IH has developed adequate IT security policies and procedures. IH has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. IH has also implemented an adequate vendor management program to assess and monitor risks associated with third-party activities.

Nothing came to our attention to indicate that IH 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. We evaluated the IH network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed perimeter controls for protecting public and partner network connections. IH utilizes firewalls to control connections with systems outside of its network as well as between the development and production environments.

IH also requires multi-factor authentication for remote access. IH servers send a unique token to the user [redacted] for verification. If the user's credentials are valid, the user is then authenticated.

IH utilized firewalls to control connections with systems outside of its network as well as between the development and production environments.

Additionally, we observed network access controls to prevent unauthorized devices from connecting to the network. If an associate needs to access a host on the internal network, IH's risk management team ensures authentication and encryption requirements are being satisfied before device approval.

Nothing came to our attention to indicate that IH has not implemented adequate controls related to network security.

C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

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.

Our review found the following controls in place:

- Controls to monitor security events throughout most of the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

The following section documents an opportunity for improvement related to IH's security event monitoring and incident response controls.

1. Wireless Event Monitoring

IH has implemented a security information and event management tool that ingests and correlates security logs from most of IH's systems and applications. However, IH is not currently monitoring wireless network activity logs. We were told that IH has developed a plan to monitor wireless activity in the near future.

IH is not currently monitoring wireless network activity logs.

NIST SP 800-53, Revision 4, states that organizations should "[monitor] and [control] communications at the external boundary of the system and at key internal boundaries within the system … ."

Failure to routinely monitor key network points increases the risks that inappropriate or malicious activity will go undetected, increasing the impact of a potential breach.

Recommendation 1

We recommend that IH implement controls to monitor wireless network activity.

IH's Response:

"IH implemented a network access control solution to monitor wireless network activity in December 2020."

OIG Comment:

In response to the draft audit report, IH provided evidence that it has implemented a network access control to monitor wireless network activity; no further action is required.

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

Our review found the following controls in place:

- Emergency change management procedures;
- A documented system change control process; and
- An established patch management process.

However, we noted the following opportunities for improvement related to IH's configuration management.

1. Security Configuration Standards

Security configuration standards are formally approved documents that list specific security settings. IH has developed tailored security configuration standards based on [redacted] benchmarks for some of the operating systems in its environment. However, standards for all of its operating systems have not been established. IH has recognized this gap and a project is in place to develop, review, and implement security configuration standards on all systems. [redacted]

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 should develop, document, and maintain a current baseline configuration of the information system.

Failure to document and approve security configuration standards for all operating platforms increases the risk that systems are not configured appropriately and left undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 2

We recommend that IH document approved security configuration standards for all operating system platforms in its technical environment.

IH's Response:

"IH has an active project to define, implement and monitor technical security configurations using industry standard benchmarks."

OIG Comment:

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

2. Security Configuration Auditing

As noted above, IH does not maintain approved security configuration standards for all of its operating system platforms, and therefore it cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings). IH is aware of the gap and has started a project to define, implement, and audit security configurations of its system utilizing tools that are already in place. [redacted]

NIST SP 800-53, Revision 4, states that an organization should 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 3

We recommend that IH 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 2 are in place.

IH’s Response:

“IH has an active project to define, implement and monitor technical security configurations using industry standard benchmarks.”

3. System Lifecycle Management

IH does not have guidance related to unsupported software.

IH conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. Our review of the scan results identified isolated incidents of missing patches; IH is actively tracking those missing patches and has established remediation dates. Documented risk exceptions are used in accordance to IH policies for any patches that cannot be applied within the required timeframe.

[redacted] The vendors of these products typically publicize information related to the product’s “end-of-life” support dates (i.e., dates when the vendor will no longer release security updates and patches). [redacted]

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 leaves information systems open to known vulnerabilities without any remediation available.

Recommendation 4

We recommend that IH develop and implement policies and procedures to ensure that unsupported software is upgraded or removed from its environment prior to the end of vendor support.

IH’s Response:

“IH is enhancing our Policy and Procedures to ensure that unsupported software is upgraded or removed from our environment prior to the end of vendor support. Where software must remain due to business or application requirements, an exception process has been implemented to track and report this risk until it can be addressed.”

APPENDIX

Independent Health

511 Farber Lakes Drive
Buffalo, NY 14221

Independent Health Association
IT General Controls Audit
2020

Management Responses

To: Martin Wiley
OPM – Office of the Inspector General
202-606-3671
Martin.Wiley@opm.gov

Subject: IH management responses to OPM recommendations

Date: February XX, 2021

Dear Mr. Wiley,
Below you will find Independent Health management responses to OPM's audit recommendations:

A. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

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.
Our review found the following controls in place:

- Controls to monitor security events throughout most of the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

The following section documents an opportunity for improvement related to IH's security event monitoring and incident response controls.

1. Wireless Event Monitoring

IH has implement a Security Information and Event Management tool that ingests and correlates security logs from most of IH's systems and applications. However, IH is not currently monitoring wireless network activity logs. We were told that IH has developed a plan to monitor wireless activity in the near future.

IH is not currently monitoring wireless network activity logs.

NIST SP 800-53, Revision 4, states that organizations should "[monitor] and [control] communications at the external boundary of the system and at key internal boundaries within the system . . . ."

Failure to routinely monitor key network points increases the risks that inappropriate or malicious activity will go undetected, increasing the impact of a potential breach.

Recommendation 1

We recommend that IH implement controls to monitor wireless network activity.

Management Response

IH implemented a network access control solution to monitor wireless network activity in December 2020.

B. 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. IH employs a team of technical personnel who manage system software configuration for the organization. We evaluated IH's management of the configuration of its computer servers and databases.
Our review found the following controls in place:

- Emergency change management procedures;
- A documented system change control process; and
- An established patch management process.

However, we noted the following opportunities for improvement related to IH's configuration management.

1. Security Configuration Standards

Security configuration standards are formally approved documents that list specific security settings. IH has developed tailored security configuration standards based on standards for some of the operating systems in its environment. However, standards for all of its operating systems have not been established. IH has recognized this gap and a project is in place to develop, review, and implement security configuration standards on all systems.

NIST SP 800-53, Revision 4, states that an organization should 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 2

We recommend that IH document approved security configuration standards for all operating system platforms in its technical environment.

Management Response

IH has an active project to define, implement and monitor technical security configurations using industry standard benchmarks.

2. Security Configuration Auditing

As noted above, IH does not maintain approved security configuration standards for all of its operating system platforms, and therefore it cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings). IH is aware of the gap and has started a project to define, implement, and audit security configurations of its system utilizing some tools that are already in place.

NIST SP 800-53, Revision 4, states that an organization should 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 3

We recommend that IH 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 2 are in place

Management Response

IH has an active project to define, implement and monitor technical security configurations using industry standard benchmarks.

Recommendation 4

We recommend that IH develop and implement policies and procedures to ensure that unsupported software is upgraded or removed from its environment prior to the end of vendor support.

Management Response

IH is enhancing our Policy and Procedures to ensure that unsupported software is upgraded or removed from our environment prior to the end of vendor support. Where software must remain due to business or application requirements, an exception process has been implemented to track and report this risk until it can be addressed.

We acknowledge and appreciate your recommendations.

John R Rodgers

Date __2/2/2021__

John Rodgers
EVP -Chief Operating Officer

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