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

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT GROUP HEALTH COOPERATIVE OF SOUTH CENTRAL WISCONSIN

Report Number 2023-ISAG-024

July 15, 2024

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Group Health Cooperative of South Central Wisconsin.

Report No. 2023-ISAG-003 **July 15, 2024**

Why Did We Conduct the Audit?

Group Health Cooperative of South Central Wisconsin (GHC) is contracted by the U.S. Office of Personnel Management (OPM) to provide health insurance benefits for Federal employees, annuitants, and their eligible dependents as part of the Federal Employees Health Benefits Program (FEHBP).

The objective of this audit performed by the OPM Office of the Inspector General was to determine if GHC has implemented adequate general and application controls to protect the confidentiality, integrity, and availability of FEHBP data processed and stored by its information systems.

What Did We Audit?

The scope of this audit included all GHC information systems operating in the general control environment where FEHBP data is processed and stored as of February 2024.

Michael R. Esser

Assistant Inspector General for Audits

What Did We Find?

Our audit of GHC's information systems general and application controls determined that:

- GHC has not developed an organization-wide Information Security Program Plan.
- GHC does not ensure individuals with specialized IT responsibilities receive technical training specific to their job function.
- GHC does not review IT policies in accordance with the frequency defined in GHC's online repository.
- GHC has not implemented multi-factor authentication for privileged user accounts.
- Terminated GHC employees continue to have logical active access to GHC systems.
- GHC has also not developed a documented process to remove inactive users.
- GHC has not developed policies and procedures for how often access codes should be changed or updated.
- Terminated GHC employees continue to have physical active access to GHC systems.
- GHC does not have an adequate vulnerability scanning process to ensure all servers are routinely scanned.
- GHC has not developed an incident response plan in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 5.
- GHC has unsupported software within its environment.
- GHC security patches were not installed within GHC's 30-day required timeframe.
- GHC's primary data center is less than 10 miles from its secondary data center.
- GHC has implemented adequate system development lifecycle controls.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information Systems Controls Audit Manual**
GAGAS	**Generally Accepted Government Auditing Standards**
GAO	**U.S. Government Accountability Office**
GHC	**Group Health Cooperative of South Central Wisconsin**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
MFA	**Multi-Factor Authentication**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of Group Health Cooperative of South Central Wisconsin's (GHC) general and application controls over its information systems operating in the general information technology (IT) control environment where Federal Employees Health Benefits Program (FEHBP) data is processed and stored as of February 2024.

The FEHBP was established by the Federal Employees Health Benefits Act (Public Law 86-382), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for Federal employees, annuitants, and their dependents. Health insurance coverage is made available through contracts with various health insurance carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

The provisions of the Federal Employees Health Benefits Act are implemented by the U.S. Office of Personnel Management (OPM) through regulations that are codified in Title 5, Chapter 1, Part 890 of the Code of Federal Regulations (CFR).

FEHBP contracts include provisions stating that an authorized representative of the Contracting Officer may use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (or its current equivalent) requirements as a benchmark for conducting audits of a health insurance carrier's information systems and may recommend that the carrier adopt a best practice drawn from NIST SP 800-53 (or its current equivalent) to information systems that directly process FEHBP data and all other information systems in the same general IT environment.

The audit was conducted pursuant to GHC's FEHBP contract CS 1828; 5 U.S.C. Chapter 89; and 5 CFR Chapter 1, Part 890. The audit was performed by OPM's Office of the Inspector General (OIG), as established and authorized by the Inspector General Act of 1978, as amended.

This was our initial audit of the information systems general and application controls at GHC. All GHC 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 were greatly appreciated.

II. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this audit was to determine if GHC has implemented adequate general and application controls over its information systems to protect the confidentiality, integrity, and availability of FEHBP data.

SCOPE AND METHODOLOGY

This audit was a performance audit conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of this audit included all GHC information systems operating in the general IT control environment where FEHBP data is processed and stored as of February 2024.

Due to resource limitations, we were not able to assess GHC's entire information systems control environment. Therefore, the scope of our work was limited to high-risk areas identified during the planning phase of our audit. Accordingly, we performed a risk assessment of GHC's information systems environment and applications during the planning phase of the audit to develop an understanding of GHC's internal controls. Using this risk assessment, additional audit steps were developed, as appropriate, to verify that the internal controls were properly designed, placed in operation, and effective.

Our audit program was based on procedures contained in the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) and NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

NIST SP 800-53 controls were selected for testing based on risk, applicability, and overall impact to the organization's IT security posture. These controls have been organized into the following audit sections:

- Enterprise Security;
- Logical Access;
- Physical Access;
- Data Center;
- Network Security;

- Security Event Monitoring and Incident Response;
- Configuration Management;
- Contingency Planning; and
- System Development Lifecycle.

For each of our audit sections, FISCAM identifies critical elements that represent tasks essential for establishing adequate controls. For each critical element, there is a discussion of the associated objectives, risks, and critical activities, as well as related control techniques and audit concerns.

NIST SP 800-53A, Revision 5 *Assessing Security and Privacy Controls in Information Systems and Organizations* includes a comprehensive set of procedures for assessing the effectiveness of security and privacy controls defined in NIST SP 800-53. We used these potential assessment methods and artifacts, where appropriate, to evaluate GHC's internal controls. This includes interviews, observations, control tests, and inspection of computer-generated data and various documents, including IT and other related organizational policies and procedures.

When our objective involved the assessment of computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable. However, due to time constraints, we did not verify the reliability of data used to complete some of our audit steps when we determined that the evidence was adequate to achieve our audit objectives.

Control tests were performed to determine the extent to which established controls and procedures are functioning as intended. Where appropriate, control tests utilized judgmental sampling methods. Results of judgmentally selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

All audit work was completed remotely, and the remote work performed included interviews of staff, documentation reviews, and testing of the general and application controls in place over GHC's information systems. The business processes reviewed are primarily located in Madison, Wisconsin.

The findings, recommendations, and conclusions outlined in this report are based on the status of information systems general and application controls in place at GHC as of February 27, 2024.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether GHC's information system general and application controls were consistent with applicable standards. Various laws,

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

- GAO's FISCAM;
- NIST SP 800-53, Revision 5;
- NIST SP 800-34, Revision 1; and
- GHC's policies and procedures.

While generally compliant with respect to the items tested, GHC was not in compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. ENTERPRISE SECURITY

Enterprise security controls include the policies, procedures, and techniques that serve as the foundation of Group Health GHC's overall IT security program. We evaluated GHC's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

GHC has not developed an organization-wide Information Security Program Plan.

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

- Formally documented risk assessment policies;
- Routine information security risk assessments; and
- Administration of routine security awareness training.

However, we identified the following opportunities for improvement related to GHC's enterprise security controls.

1. Information Security Program Plan

An Information Security Plan defines the security requirements for an organization and describes the controls in place for meeting those requirements. We reviewed GHC's IT Security policies to determine the existence of an Information Security Program Plan. However, no document or group of documents demonstrated the establishment of an Information Security Program Plan for GHC.

NIST SP 800-53, Revision 5, control PM-1 states that the organization should develop and disseminate an organization-wide information security program plan that provides an overview of the requirements for the security program, describes security program management controls and common controls, identifies roles and responsibilities, and is approved by a senior official.

Failure to establish an Information Security Program Plan increases the risk that a security program will not be organized to fulfill security requirements.

Recommendation 1

We recommend that GHC develop an organization-wide Information Security Program Plan.

GHC's Response:

"We have an initiative underway to document our Information Security Plan."

OIG Comments:

As a part of the audit resolution process, GHC should provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence that it has fully implemented this recommendation. **This statement also applies to the subsequent recommendations in this audit report that GHC agrees to implement**.

2. Role-Based Training

GHC requires annual IT security and privacy awareness training for all employees. However, GHC does not ensure individuals with specialized IT responsibilities receive technical training specific to their job function.

NIST SP 800-53, Revision 5, control AT-3 states that the organization should provide role-based security and privacy training to personnel with the following duties: systems engineers, software developers, information security officers, system owners, network and database administrators, and other IT-related positions.

Failure to ensure role-based technical training for IT staff increases the risk that individuals are not adequately prepared to identify and address constantly evolving IT threats.

Recommendation 2

We recommend that GHC require specialized training for employees with significant security roles and responsibilities.

GHC's Response:

"A module is being set up in our LMS and will be assigned to appropriate IT staff starting in June of 2024."

3. IT Policy Review

GHC has a policy review process that requires that the Information Technology division review departmental policies based on the frequency specified in GHC's online document repository. Policies within the repository are required to be reviewed annually or bi-annually. However, out of the six GHC IT Security policies provided to OIG, none were reviewed in accordance with the frequency defined in GHC's online repository.

GHC's Policy Review document states that "Under direction from the Chief Information Officer, the appropriate experts in the Information Technology division will review departmental polices on the frequency specified in the Review Cycle field for each policy on PolicyHub."

Failure to review policies increases the risk that GHC policies will be outdated and ineffective in managing risk.

Recommendation 3

We recommend that GHC review policies in accordance with its organization defined frequency.

GHC's Response:

"A new process to check on policies on a monthly basis and make sure all are updated has been put into place."

B. LOGICAL ACCESS

Logical access controls include the policies, procedures, and techniques used to detect and prevent unauthorized logical access to information systems or modification, loss, and disclosure of sensitive data. We evaluated the logical access controls protecting sensitive data on GHC's network environment and applications supporting the FEHBP claims processing business function.

GHC does not implement multi-factor authentication for privileged user accounts.

The controls observed during this audit included, but were not limited to:

- Procedures for appropriately granting and removing logical access to applications and software resources;
- Logical access is granted using the principle of least privilege; and
- Limits for consecutive invalid logon attempts are enforced.

However, we identified the following opportunities for improvement related to GHC's logical access controls.

1. Privileged User Authentication

GHC leverages Active Directory credentials to manage access for both non-privileged and privileged accounts. Privileged users have a separate account created for administrator responsibilities, which only requires a username and password for

authentication. However, after analyzing GHC's logical access policies to identify if GHC has established documented multi-factor authentication (MFA) requirements for privileged accounts, we identified that GHC does not require MFA for privileged users.

NIST SP 800-53, Revision 5, control IA-2 states that the organization should implement MFA for access to privileged accounts.

Failure to implement MFA to access privileged accounts increases the risk that threat actors may access privileged credentials.

Recommendation 4

We recommend that GHC implement MFA for privileged user accounts.

GHC's Response:

"We are currently evaluating solutions for privileged user accounts."

2. Removal of System Access

We compared a list of employees terminated within the last two years to a list of active accounts. To ensure terminated GHC employees no longer have system access, GHC performs bi-annual reviews. However, according to our analysis of 769 terminated employees, 25 employees continued to have active access to GHC systems.

NIST SP 800-53, Revision 5, control AC-2 states that organizations should "Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria] … ."

Failure to properly remove terminated user's accounts increases the risk of unauthorized access to confidential data and systems.

Recommendation 5

We recommend that GHC improve its auditing process to ensure access is being properly removed and terminated users no longer have logical access to systems.

GHC's Response:

"GHC performs a quarterly process to review and remove deactivated accounts. In addition to this a process to disable inactive accounts after 60 days has been established."

3. Inactive Accounts

During our Subject Matter Expert meetings, GHC stated that a defined time for disabling inactive accounts has not been established by the organization. GHC has also not developed a documented process to remove inactive users.

NIST SP 800-53, Revision 5, control AC-2 states that organizations should "Disable accounts within [Assignment: organization-defined time period] when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for [Assignment: organization-defined time period]."

Failure to implement an organization-defined time period for the disabling of inactive accounts increases the risk that unauthorized users will be able to access and attack GHC's systems and environment.

Recommendation 6

We recommend that GHC develop and implement policies and procedures for disabling inactive users.

GHC's Response:

"A process to disable inactive accounts after 60 days has been set up."

C. PHYSICAL ACCESS

Physical access controls include the policies, procedures, and techniques used to prevent or detect unauthorized physical access to facilities which contain information systems and sensitive data. We evaluated the controls protecting physical access to GHC's facilities and data centers.

The controls observed during this audit included, but were not limited to:

- Physical access to the headquarters facility is controlled using a badge access system;
- Access to facilities is provisioned based on least privilege; and
- The main employee entrance is monitored with security cameras.

However, we identified the following opportunities for improvement related to GHC's physical access controls.

1. Shared Access Codes

GHC uses access codes to enter network closets within its facilities; however, there are no policies in place that mandate when access codes should be changed or updated.

GHC has not developed policies and procedures that define how often access codes should be changed or updated.

NIST SP 800-53, Revision 5, control PE-3 states that the organization should "Change combinations and keys [at an organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated."

Failure to change shared access codes can give terminated employees unauthorized access to an organization's systems.

Recommendation 7

We recommend that GHC develop and implement policies and procedures that define how often access codes should be changed or updated.

GHC's Response:

"GHC will install a card reader and electric door strike to allow the door to be controlled through the access control system instead of the codes."

2. Disabling and Removing User Accounts

We compared a list of employees terminated within the last two years to a list of active accounts. During our review we identified 18 terminated employees out of 769 who

retained physical access. We reviewed GHC's policies and procedures; however, disabling accounts within a specific time frame has not been defined.

NIST SP 800-53, Revision 5, control AC-2 states that organizations should "Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organization policy; or (d) Have been inactive for [Assignment: organization-defined time period]."

Failure to disable and remove terminated employees increases the risk that unauthorized users can access accounts and compromise organizational systems.

Recommendation 8

We recommend that GHC disable and remove inactive accounts identified during this audit.

GHC's Response:

"We have confirmed that all accounts identified were disabled."

Recommendation 9

We recommend that GHC update its current procedures to ensure the audits of physical access lists are reviewed for appropriateness and action is taken to disable and remove inactive accounts.

GHC's Response:

"Facilities and HR are working together on a process for HR to supply a list of termed staff on a monthly basis which will be compared to the card access system."

D. DATA CENTER

Data center controls include the policies, procedures, and techniques used to protect information systems from environmental damage and provide network resiliency. We evaluated the data center controls at GHC's primary and back-up data centers.

GHC has implemented adequate data center controls.

The controls observed during this audit included, but were not limited to:

- Data center physical access is monitored;
- Environmental controls maintain temperature and humidity; and

- Alternate telecommunication services provide network redundancy.

Nothing came to our attention to indicate that GHC has not implemented adequate data center controls.

E. NETWORK SECURITY

Network security controls include the policies, procedures, and techniques used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. We evaluated GHC's controls related to network design, data protection, and systems monitoring.

GHC does not have an adequate vulnerability scanning process to ensure all servers are routinely scanned.

The controls observed during this audit included, but were not limited to:

- Perimeter controls secure connections to external networks;
- Network connections are denied by default and permitted by exception; and
- Network access controls prevent unauthorized devices from connecting to the internal network.

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

1. Vulnerability Management

As a part of this audit, GHC conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network on our behalf. We chose a judgmental sample of 152 servers from a universe of 456 and 20 workstations and laptops from a universe of 1,424. The sample included a variety of system functionality and operating systems across production, test, and development environments. The sample was judgmentally selected from systems that store and/or process FEHBP data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population. The specific vulnerabilities that we identified were provided to GHC in the form of an audit inquiry but will not be detailed in this report. GHC was aware of the vulnerabilities and is in the process of developing plans to remediate the issues we found.

NIST SP 800-53, Revision 5, control RA-5 states that the organization should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

Failure to scan all systems increases the risk that vulnerabilities will go undetected and could be exploited.

Recommendation 10

We recommend that GHC improve its vulnerability scanning process to ensure that all servers are routinely scanned, and vulnerabilities are tracked to remediation.

GHC's Response:

"Scanning is being performed weekly. GHC-SCW's vulnerability management and remediation program is under development and will incorporate OIGs recommendations."

Recommendation 11

We recommend that GHC continue to remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

GHC's Response:

"GHC-SCW's vulnerability management and remediation program is under development and will incorporate OIGs recommendations."

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

GHC does not have a documented incident response plan.

Security event monitoring controls include the policies, procedures, and techniques used for 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 controls include the policies, procedures, and techniques used to establish and implement an incident response plan which defines roles and responsibilities, response procedures, training, and reporting. We evaluated GHC's controls related to event log collection and security incident detection, response, and reporting.

The controls observed during this audit included, but were not limited to:

- Security event monitoring throughout the network;
- A log analysis process; and
- Procedures for analyzing security events.

However, we identified the following opportunity for improvement related to GHC's security event monitoring and incident response controls.

1. Incident Response Plan

GHC performs event log analysis and conducts routine incident response testing. However, GHC does not have a documented incident response plan.

NIST SP 800-53 Revision 5, control IR-4 states that the organization should "Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery … ."

Failure to have a documented incident response plan increases the risk that the incident response team could be delayed or ineffective when responding to security events.

Recommendation 12

We recommend that GHC develop and implement an incident response plan that includes guidance on preparation, detection and analysis, containment, eradication, and recovery.

GHC's Response:

"GHC does have an Incident Response Plan document and we are currently working on updating it."

OIG Comments:

During audit fieldwork, we were provided with an incident response diagram; however, the intent of the recommendation is for GHC to formally document an incident response plan to include the elements described in NIST SP 800-53 Revision 5, control IR-4.

G. CONFIGURATION MANAGEMENT

Configuration management controls include the policies, procedures, and techniques used to develop, implement, and maintain secure, risk-based system configurations and ensure that systems are configured according to these standards. We evaluated GHC's configuration management of its end-user devices, servers, and databases.

GHC has unsupported software within its environment.

The controls observed during this audit included, but were not limited to:

- Established configuration management policy;

- Documented system configuration change approvals; and
- An adequate patch management policy.

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

1. Security Configuration Auditing

GHC maintains approved security baselines for all operating systems, however, it has not developed a process to routinely audit systems to ensure the security settings remain in compliance with the approved baselines.

NIST SP 800-53, Revision 5, CM-6 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 perform routine security configuration auditing increases the risk that systems with unsecure configurations will go undetected, leaving the system vulnerable to a cyber-attack.

Recommendation 13

We recommend that GHC implement a routine process to audit security configuration settings of its servers to ensure compliance with approved security configuration settings.

GHC's Response:

"We are finalizing our formal server hardening checklist/policy as the first step to this. Once that is complete, we can create the audit process."

2. Patch Management

GHC conducted vulnerability and configuration compliance scans on a sample of servers in its network environment on our behalf. GHC provided a policy that mandates a 30-day timeframe for remediating all patches within its environment. However, our review of the scan results indicated that various security patches were not installed within the 30-day timeframe. In response to this finding, we were told that GHC has attempted to improve its patch management process through manual patching and patching is now being managed monthly. GHC is also developing automated patching procedures. For

the security patches that cannot be managed via automation, GHC will continue to track and update patches manually.

NIST SP 800-53, Revision 5, control SI-2 states that the organization should "Install security-relevant software and firmware updates within [the organization-defined time period] of the release of the updates … ."

Failure to install patches in a timely manner increases the risk that threat actors could exploit system weaknesses for malicious purposes.

Recommendation 14

We recommend that GHC improve its patching process to ensure all patches are remediated within the organization's mandated timeframe.

GHC's Response:

"We are in the process of updating our policies and procedures related to patching."

3. Unsupported Software

During our vulnerability scanning exercise, we identified numerous instances of unsupported software in GHC's IT environment. GHC has not developed or implemented procedures that define how unsupported software should be handled within the organization. In response to this finding, GHC stated that there is ongoing effort to establish more robust scanning practices and to develop better asset inventory documentation that would identify and address unsupported software.

NIST SP 800-53, Revision 5, control SA-22 states that the organization should "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer" or obtain extended support.

Failure to remove unsupported software from the IT environment increases the risk that components which are no longer receiving critical software patches will be attacked.

Recommendation 15

We recommend that GHC develop and implement policies and procedures which define how unsupported software should be handled before the end-of-life date.

GHC's Response:

"A formal software asset management program is underway which will include the policies and procedures for this."

H. CONTINGENCY PLANNING

Contingency planning controls include the policies, procedures, and techniques that ensure continuity and recovery of critical business operations and the protection of data in the event of a service impacting incident. We evaluated GHC's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when service impacting events occur.

GHC's primary data center is less than 10 miles from its secondary data center.

The controls observed during this audit included, but were not limited to:

- Documented business continuity and disaster recovery plans;
- Recovery priorities for system recovery; and
- A documented disaster recovery testing policy.

However, we identified the following opportunity for improvement related to GHC's contingency planning controls.

1. Primary and Secondary Data Center Proximity

GHC's primary data center is less than 10 miles from its secondary data center, which could allow both data centers to be susceptible to the same threats. GHC has not performed a risk assessment of its primary and secondary data centers to determine if it is acceptable to locate the data centers in such close proximity.

NIST SP 800-53, Revision 5, control CP-6 states that the organization should "Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats."

NIST SP 800-34, Revision 1, states that the organization should have alternate processing facilities that "provide a location for an organization to resume system operations in the event of a catastrophic event that disables or destroys the systems primary facility."

Failure to perform a risk assessment defining an appropriate distance between the primary and secondary data centers increases the risk that a single event could disrupt both data centers simultaneously.

Recommendation 16

We recommend that GHC conduct a risk assessment to identify the risks involved in having the primary and secondary data centers in close proximity and then make a determination if the risk is acceptable.

GHC's Response:

"We will continue to assess our data center strategy. As we transition more systems to cloud and hosting models, we may explore opportunities to increase the distance between our data centers in the future. This will include planning for the associated costs of relocating one of the data centers."

I. SYSTEM DEVELOPMENT LIFECYCLE

System development lifecycle controls include the policies, procedures, and techniques related to the secure and controlled internal development of software supporting claims adjudication and sensitive web applications. We evaluated GHC's software development and change control policies and procedures and controls related to secure software development.

GHC has implemented adequate software development procedures.

The controls observed during this audit included, but were not limited to:

- Documented software change management policies;
- Documented software development procedures; and
- Application change review and approval process.

Nothing came to our attention to indicate that GHC has not implemented adequate system development lifecycle controls.

APPENDIX

GHC Draft Report Responses - 2024

May 23, 2024

#	Section	OIG Recommendation	GHC Remediation Notes
1	Enterprise Security	We recommend that GHC develop an organization-wide Information Security Program Plan	We have an initiative underway to document our Information Security Plan.
2	Enterprise Security	We recommend that GHC require specialized training for employees with significant security roles and responsibilities.	A module is being set up in our LMS and will be assigned to appropriate IT staff starting in June of 2024.
3	Enterprise Security	We recommend that GHC review policies in accordance with its organization defined frequency.	A new process to check on policies on a monthly basis and make sure all are updated has been put into place.
4	Logical Access	We recommend that GHC implement MFA for privileged user accounts.	We are currently evaluating solutions for privileged user accounts.
5	Logical Access	We recommend that GHC improve its auditing process to ensure access is being properly removed and terminated users no longer have logical access to systems.	GHC performs a quarterly process to review and remove deactivated accounts. In addition to this a process to disable inactive accounts after 60 days has been established.
6	Logical Access	We recommend that GHC develop and implement policies and procedures for disabling inactive users.	A process to disable inactive accounts after 60 days has been set up.
7	Physical Access	We recommend that GHC develop and implement policies and procedures that define how often access codes should be changed or updated.	GHC will install a card reader and electric door strike to allow the door to be controlled through the access control system instead of the codes.
8	Physical Access	We recommend that GHC disable and remove inactive accounts identified during this audit.	We have confirmed that all accounts identified were disabled.
9	Physical Access	We recommend that GHC update its current procedures to ensure the audits of physical access lists are reviewed for appropriateness and action is taken to disable and remove inactive accounts.	Facilities and HR are working together on a process for HR to supply a list of termed staff on a monthly basis which will be compared to the card access system.
10	Network Security	We recommend that GHC improve its vulnerability scanning process to ensure that	Scanning is being performed weekly. GHC-SCW's vulnerability management and remediation program

#	Section	OIG Recommendation	GHC Remediation Notes
		all servers are routinely scanned, and vulnerabilities are tracked to remediation.	is under development and will incorporate OIGs recommendations.
11	Network Security	We recommend that GHC continue to remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.	GHC-SCW's vulnerability management and remediation program is under development and will incorporate OIGs recommendations.
12	System Event Monitoring and Incident Response	We recommend that GHC develop and implement an incident response plan that includes guidance on preparation, detection and analysis, containment, eradication, and recovery.	GHC does have an Incident Response Plan document and we are currently working on updating it.
13	Configuration Management	We recommend that GHC implement a routine process to audit security configuration settings of its servers to ensure compliance with approved security configuration settings.	We are finalizing our formal server hardening checklist/policy as the first step to this. Once that is complete, we can create the audit process.
14	Configuration Management	We recommend that GHC improve its patching process to ensure all patches are remediated within the organization's mandated timeframe	We are in the process of updating our policies and procedures related to patching.
15	Configuration Management	We recommend that GHC develop and implement policies and procedures which define how unsupported software should be handled before the end-of-life date.	A formal software asset management program is underway which will include the policies and procedures for this.
16	Contingency Planning	We recommend that GHC conduct a risk assessment to identify the risks involved in having the primary and secondary data centers in close proximity and then make a determination if the risk is acceptable.	We will continue to assess our data center strategy. As we transition more systems to cloud and hosting models, we may explore opportunities to increase the distance between our data centers in the future. This will include planning for the associated costs of relocating one of the data centers.

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: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100