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 GOVERNMENT EMPLOYEES HEALTH ASSOCIATION, INC.

Report Number 1B-31-00-18-033
March 1, 2019

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Government Employees Health Association, Inc.

Report No. 1B-31-00-18-033 **March 1, 2019**

Why Did We Conduct The Audit?

The Government Employees Health Association (GEHA) 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 GEHA's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by GEHA to process and store data related to medical encounters and insurance claims for FEHBP members. The audit also included general IT controls managed by GEHA.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of GEHA determined:

- GEHA has an adequate risk assessment methodology in place. However, GEHA could improve its security management by both establishing a [redacted] and tracking technical staff training.
- GEHA has implemented logical and physical access policies and controls for its applications and facilities.
- GEHA could improve its network security posture by [redacted], documenting and reviewing its [redacted] standards, and [redacted]
- GEHA does not have an updated configuration management policy. In addition, GEHA is [redacted].
- GEHA conducts vulnerability scanning of its server network. However, it does not have policies and procedures in place to [redacted].
- GEHA maintains disaster recovery and business continuity plans and has implemented controls to protect against service disruption.
- GEHA has implemented controls supporting the processing and output of claims. However, GEHA could improve the controls for processing paper claims.

ABBREVIATIONS

CMDB	**Configuration Management Database**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GEHA	**Government Employees Health Association, Inc.**
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**
Q	**Quarter**
[redacted]	[redacted]

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 the Government Employees Health Association, Inc. (GEHA).

The audit was conducted pursuant to FEHBP contracts CS 1063; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations 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 Federal Employees Health Benefits Act, enacted on September 28, 1959, established the FEHBP to provide health insurance benefits for Federal employees, annuitants, and qualified dependents. OPM implements the provisions of the Federal Employees Health Benefits Act through regulations codified in 5 Code of Federal Regulations Chapter 1, Part 890. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our fourth audit of the information technology (IT) general and application controls at GEHA. The previous audits resulted in findings and recommendations documented in Report No. 31-00-99-008, dated September 30, 1999; Report No. 1B-31-00-04-090, dated January 13, 2006; and Report No. 1B-31-00-11-066 dated August 9, 2012. All findings from the previous audits have been closed.

All GEHA 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. We greatly appreciated their positive attitude and helpfulness throughout the audit.

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

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to GEHA's claims processing system.

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of GEHA'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 GEHA'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 GEHA to process medical insurance claims and/or store the data of GEHA members. The business processes reviewed are primarily located in Kansas City, Missouri.

The onsite portion of this audit was performed in April and May of 2018. We completed additional audit work before and after the on-site visits 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 GEHA as of June 2018.

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

- Gathered documentation and conducted interviews;
- Reviewed GEHA's business structure and environment;
- Performed a risk assessment of GEHA's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's 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 GEHA's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- Title 5 of the Code of Federal Regulations;
- U.S. Government Accountability Office's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Information Security;
- NIST SP 800-14, 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, Guidelines on Firewalls and Firewall Policy;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

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

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether GEHA's practices were consistent with applicable standards. While generally compliant with respect to the items tested, GEHA was not in complete compliance with all standards, as described in Section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

Security management encompasses the policies and procedures that are the basis of GEHA's overall IT security program. We evaluated GEHA's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls. In addition, we reviewed the human resources policies and procedures related to hiring, training, transferring, and terminating employees.

GEHA has developed a detailed risk management methodology and has documented remediation plans to address weaknesses identified during risk assessments. GEHA also maintains adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

The sections below document areas for improvement related to GEHA's security management controls.

1. Asset Inventory

[redacted] Currently, various internal groups use and manage multiple tools [redacted]

GEHA could improve its enterprise security by maintaining a centralized inventory of its IT environment.

FISCAM states, "To implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their systems. Without one, the entity cannot effectively manage [information security] controls across the entity."

Failure to maintain a complete inventory increases the risk that security processes omit systems and those systems are able to reside on the network with significant security vulnerabilities.

Recommendation 1

We recommend that GEHA [redacted] and maintain a comprehensive inventory of all of the systems and software in its technical environment.

GEHA's Response:

"GEHA acknowledges the need to have a comprehensive asset inventory in place for all systems and software within our environment. [redacted] ***During Q4 2017 to Q1 2018 we established an enhanced strategy for IT Asset Management and modified fulfillment, configuration, and deployment procedures to standardize Asset Management of physical hardware. This strategy will be operationalized with CMDB/Asset Management Phase II which is target to begin late Q3 and complete by the end of 2018.***

GEHA will be establishing a standardized Software Asset Management . . . process as part of the Asset Management/CMDB Program. Due to the nature of [Software Asset Management] and the breadth of the program we are looking into creating a separate enterprise-level project for Software Asset Management so that the full lifecycle and all stakeholders are accounted for. It is estimated that [Software Asset Management] will begin in 2019 and may take the year and beyond to complete. It will also have defined phases as we have utilized for Phase I and Phase II of our [CMDB]/Asset Management Program.

In addition, GEHA utilizes [redacted] ***to scan the environment*** [redacted] ***Hardware and software assets captured in the scan results are evaluated by the security team. Unauthorized hardware and software are escalated to the attention of GEHA's*** [redacted]

Also, [redacted] ***system. This information is refreshed*** [redacted] ***as part of the*** [redacted] ***business continuity planning and/or as new solutions are on-boarded in to the environment. Tracking enterprise application systems in the*** [redacted] ***system supports business continuity, disaster recovery, findings management and risk reporting."***

OIG Comments:

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

2. Background Check Process

GEHA performs background checks on new and returning employees that include verification of education and prior employment histories, and searches of criminal and multi-state sex offender registries. However, this process does not include performing a check against OPM's debarment list.

Title 5 of the Code of Federal Regulations states, "A debarred provider is not eligible to receive payment, directly or indirectly, from FEHBP funds for items or services furnished to a covered individual on or after the effective date of the debarment." Failure to check possible hires against the OPM debarment list increases the risk of debarred individuals accessing sensitive information, influencing claims adjudication, and being indirectly paid with FEHP funds.

Recommendation 2

We recommend that GEHA reevaluate the elements included in its background check process to ensure GEHA does not employ individuals debarred by OPM.

GEHA's Response:

"We concur with this recommendation. The [redacted] team expanded the background check program to include the OPM Debarment list effective May 14, 2018."

OIG Comments:

In response to our draft audit report, GEHA has provided evidence that an updated background check process has been implemented. No further action is required.

3. Specialized Training

GEHA requires all employees with technical responsibilities to maintain relevant certifications including fulfillment of the continuing professional education requirements.

However, GEHA's current tools do not have the ability to track employee compliance with this requirement. GEHA plans to implement functionality in its human resource management system to track employee's training hours.

NIST SP 800-53, Revision 4, states, "Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions."

Failure to monitor compliance with the education requirement increases the risk that employees will not have the current information, skills, and tools to solve evolving IT threats and issues.

Recommendation 3

We recommend that GEHA implement a process to monitor the technical staff's certification renewals and continuing professional education hours.

GEHA's Response:

"GEHA recognizes the need to ensure that appropriate education and training opportunities are provided to ensure that technical staff sustain knowledge and skillset in accordance with job responsibilities. Management works with staff to define annual training plans as part of employee performance reviews and department budgets include funding for identified training and/or certification courses.

On October 1, 2018 GEHA is implementing the [redacted] . . . platform. The [redacted] platform includes a learning and development module that will be utilized to track and maintain individual training, certification and continuing professional education . . . status.

Management will define and implement a [redacted] to specify requirements and expectations for routine technical training tailored to any position that has privileged or specialized IT, security and/or operational responsibilities as part of their job role.

The estimated completion date is end of Q4 2018."

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 at GEHA's facilities and datacenters. We also examined the logical access controls protecting sensitive data on GEHA's network environment and applications. The access controls observed during this audit include, but were not limited to:

- Procedures for appropriately granting, adjusting, and removing physical access to facilities and datacenters; and
- Procedures for appropriately granting, adjusting, and removing logical access to applications and software resources.

GEHA has adequate policies and procedures to control physical and logical access to its systems and facilities.

Nothing came to our attention to indicate that GEHA has not implemented adequate controls over its access control process.

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 GEHA's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit. We observed the following controls in place:

- Preventive controls at the [redacted]
- Security event monitoring throughout the network; and
- A documented incident response program.

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

1. [redacted]

GEHA does not have controls in place to prevent [redacted]

[redacted]

Recommendation 4

We recommend that GEHA implement [redacted]

GEHA's Response:

"GEHA acknowledges and agrees with the recommendation and is working to [redacted]

Although GEHA is committed to improving our [redacted]

The estimated implementation date for [redacted]

2. Documented Firewall Policy and [redacted]

GEHA has firewalls [redacted] However, GEHA has not formally documented a policy [redacted] Maintaining an approved firewall policy would enable GEHA [redacted]

NIST SP 800-41, Revision 1, states "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies." NIST SP 800-41, Revision 1, also explains that rulesets should be reviewed or tested periodically to make sure that the firewall rules comply with the organization's policies.

Failure to document an approved firewall policy increases the risk that the firewall does not properly manage network traffic. Additionally, failure to regularly audit the firewall configurations against an approved firewall policy or configuration standard increases the risk that the firewalls could be compromised and that rules exist which allow unacceptable or unneeded network traffic.

Recommendation 5

We recommend that GEHA document and approve a firewall policy [redacted]

GEHA's Response:

"GEHA agrees with the recommendation and is in the process of documenting our firewall [redacted]. Management has [redacted] to perform an [redacted] assessment of all firewall configurations as well as provide [redacted]

The estimated completion date is the end of [redacted]

Recommendation 6

We recommend that GEHA perform routine audits of its [redacted]

Note – this recommendation cannot be implemented until the controls from the preceding Recommendation 5 are in place.

GEHA's Response:

"GEHA agrees with this recommendation. Management has [redacted] aligned with industry best practice and GEHA's security control framework.

Management will establish a process to ensure that [redacted].

The estimated completion date is the end of [redacted]

3. [redacted]

GEHA has implemented [redacted] However, there [redacted]

[redacted]

[redacted]

Recommendation 7

We recommend that GEHA [redacted].

GEHA's Response:

"Although next-generation [redacted] ***GEHA acknowledges and agrees with the recommendation and is working to define and implement a network security roadmap that will include the follow key initiatives:***

A. Core Upgrade: Establishing the foundation to successfully implement [redacted]

B. Enhanced [redacted] ***Design: Leverage*** [redacted]

C. Management Zone: [redacted]

D. [redacted] ***Inspection:*** [redacted]

The estimated completion date is the end of [redacted]***."***

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. We evaluated GEHA's management of the configuration of its servers and databases. Our review identified the following controls in place:

- A formal change approval process; and
- Vulnerability scanning procedures.

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

1. Configuration Management Policies

GEHA has a configuration management policy requiring its endpoints be securely configured. However, the policy was [redacted]. An updated version of the policy is in progress but has not been approved.

GEHA has defined configuration management policies; however, these have not been updated recently.

NIST SP 800-53, Revision 4, requires an organization to develop a configuration management policy "that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance."

Failure to keep configuration management policies current weakens the security controls surrounding an environment; the outdated roles, responsibilities, procedures, and compliance requirements increase the risk that a system can be successfully exploited and sensitive data extracted.

Recommendation 8

We recommend that GEHA update and approve its corporate configuration management policies.

GEHA's Response:

"GEHA agrees with this recommendation. Management will review and update the configuration management policies.

The estimated completion date is [redacted].”

2. [redacted]

GEHA does not have [redacted] in its environment. GEHA has the ability to perform [redacted] on its systems using [redacted]

[redacted]

[redacted]

Recommendation 9

[redacted]

GEHA’s Response:

“GEHA agrees with this recommendation. [redacted]

The estimated completion date is [redacted].”

Recommendation 10

We recommend that GEHA [redacted]

Note – this recommendation cannot be implemented until the controls from the preceding Recommendation 9 are in place.

GEHA's Response:

"GEHA agrees with this recommendation. Management will leverage implemented technical solutions [redacted]

[redacted]

GEHA will develop and implement an audit program [redacted]

3. Vulnerability Management

GEHA routinely conducts [redacted] scans on all servers in its network environment. However, [redacted]

As a part of our fieldwork, we independently conducted vulnerability scans on select systems in GEHA's environment. [redacted]

FISCAM states, "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective." Additionally, NIST SP 800-53, Revision 4, requires organizations to remediate legitimate vulnerabilities identified in information systems and hosted applications.

Failure to remediate vulnerabilities in a timely manner increases the risk that bad actors could exploit system weaknesses for malicious purposes.

Recommendation 11

We recommend that GEHA review its patch management policies and procedures [redacted]

GEHA's Response:

"GEHA partially agrees with this recommendation. Management has implemented a policy and process [redacted] and [redacted] (e.g., [redacted]) through a [redacted]. In addition GEHA's environment is scanned [redacted] using the [redacted]. Issues and vulnerabilities identified are escalated to the [redacted] and are remediated according to [redacted] t policy. The [redacted] to discuss vulnerability issues and patch compliance status.

Management recognizes that the [redacted] platforms are currently patched through [redacted] and will work to update current policy and process to ensure these systems are updated on a regular patch schedule.

The estimated completion date is the end of [redacted]

4. Unsupported Software

[redacted] The vendors of these products typically publicize information [redacted] Having unsupported software leaves GEHA systems vulnerable to infiltration attempts.

We found instances of unsupported software in GEHA's IT environment.

FISCAM states "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 remove unsupported software increases the risk that bad actors could exploit system weaknesses for malicious purposes.

Recommendation 12

We recommend that GEHA upgrade [redacted]

GEHA's Response:

"GEHA agrees with this recommendation. Management will ensure that the inventory and necessary remediation steps to [redacted]

The estimated completion date is the end of [redacted]

E. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of GEHA's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Contingency plan tests; and
- Emergency response procedures.

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

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting GEHA's claims adjudication process. This included a review of the following processes related

to claims adjudication: application configuration management, claims processing, enrollment, and provider debarment.

1. **Application Configuration Management**

   We evaluated the policies and procedures governing application development and change control for GEHA's claims processing systems.

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

   - Policies and procedures that allow modifications to be tracked throughout the change process are implemented;
   - Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and
   - A group independent from the software developers moves code between development and production environments to ensure separation of duties.

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

2. Claims Processing System

   We evaluated the business process controls associated with GEHA's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that GEHA has implemented policies and procedures to help ensure:

   - Adequate controls over the processing and output of claims;
   - Quality assurance reviews of claims processing; and
   - Tracking of electronic claims and files through the adjudication process.

   The section below documents one opportunity for improvement related to the claims processing controls.

Paper Claims Tracking and Storage

During our walk-through of the claims processing workflow we noted two issues with incoming paper claims. First, GEHA does not have a process to verify that every claim received in the mailroom is scanned and input into the claims processing system.

FISCAM requires that "Procedures should be established to reasonably assure that all source documents (paper or electronic form) have been entered and accepted to create a valid transaction." Failure to verify the system inputs increases the risk that received paper claims could be unaccounted for, or missing.

Second, paper claims are currently stored in a room [redacted] While there are some employee positions that require access to this information, not everyone in the same open area needs access to this sensitive information and there are no physical controls to separate the two areas.

NIST SP 800-53, Revision 4, states that the "organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." Failure to restrict access to the claims storage area increases the risk that unauthorized employees can gain access to sensitive data contained in the room.

At the time of the audit, [redacted] will be responsible for incoming claim sorting, scanning, and data entry functions. GEHA plans to complete this change within the year.

Recommendation 13

We recommend that GEHA verify that the new contractor has controls to ensure that all incoming claims are properly input for processing and that physical storage of the paper claims implements the principle of least privilege.

GEHA's Response:

"GEHA uses a third party vendor for all paper claims, intake and storage. The vendor [redacted]

[redacted]

3. Enrollment

We evaluated GEHA's procedures for managing its member enrollment database. Enrollment information is received either electronically or in paper format, and loaded into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately and completely.

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

4. Debarment

We evaluated GEHA's procedures for managing its debarred provider database. GEHA has documented procedures for reviewing provider files for debarred or suspended providers. The OPM debarment list is downloaded monthly and uploaded into GEHA's claims system. If a debarred provider is identified in the claims processing system, a hold is placed on all claims for that debarred provider. When a new claim with a debarred provider is received, the member is notified with a form letter describing that after 15 days no additional claims will be paid per OPM guidelines.

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

APPENDIX

September 26, 2018

Mr. [redacted] Auditor-In-Charge
Information Systems Audits Group
Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW Room 6400
Washington, DC 20415-1100

Mr. [redacted]:

We have completed our review of the OIG draft report for the information technology audit of Government Employees Health Association, Inc. (GEHA) dated August 1, 2018. We have included our responses for each audit area within the OIG report draft.

Security Management – Asset Inventory
OIG Finding:
[redacted]
Currently, various internal groups use and manage multiple tools [redacted]

Recommendation 1:
We recommend that GEHA [redacted] and maintain a comprehensive inventory of all the systems and software in its technical environment.

GEHA Response:
GEHA acknowledges the need to have a comprehensive asset inventory in place for all systems and software within our environment. [redacted]

[redacted]. During Q4 2017 to Q1 2018 we established an enhanced strategy for IT Asset Management and modified fulfillment, configuration, and deployment procedures to standardize Asset Management of physical hardware. This strategy will be operationalized with CMDB/ Asset Management Phase II which is target to begin late Q3 and complete by the end of 2018

GEHA will be establishing a standardized Software Asset Management (SAM) process as part of the Asset Management/CMDB Program. Due to the nature of SAM and the breadth of the program we are

looking into creating a separate enterprise-level project for Software Asset Management so that the full lifecycle and all stakeholders are accounted for. It is estimated that SAM will begin in 2019 and may take the year and beyond to complete. It will also have defined phases as we have utilized for Phase I and Phase II of our Configuration Management Database (CMDB)/Asset Management Program.

In addition, GEHA utilizes [redacted] to scan the environment [redacted]. Hardware and software assets captured in the scan results are evaluated by the security team. Unauthorized hardware and software are escalated to the attention of GEHA's [redacted]

Also, [redacted] system. This information is refreshed [redacted] as part of the [redacted] and business continuity planning and/or as new solutions are on-boarded in to the environment. Tracking enterprise application systems in the [redacted] system supports business continuity, disaster recovery, findings management and risk reporting.

Security Management – Background Check Process

OIG Finding:

GEHA performs background checks on new and returning employees that include verification of education and prior employment histories, and searches of criminal and multi-state sex offender registries. However, this process does not include performing a check against OPM's debarment list.

Recommendation 2:

We recommend that GEHA reevaluate the elements included in its background check process to ensure GEHA does not employ individuals debarred by OPM.

GEHA Response:

We concur with this recommendation. [redacted] team expanded the background check program to include the OPM Debarment list effective May 14, 2018.

Attached is a report from our background system, [redacted] (refer to #2 Attachment). This report shows that the OIG/GSA Debarment list has been included in the background check process for those background checks initiated since May 15, 2018.

Security Management – Specialized Training

OIG Finding:

GEHA requires all employees with technical responsibilities to maintain relevant certifications including fulfillment of the continuing professional education requirements. However, GEHA's current tools do not have the ability to track employee compliance with this requirement. GEHA plans to implement functionality in its human resource management system to track employee's training hours.

Recommendation 3:

We recommend that GEHA implement a process to monitor the technical staff's certification renewals and continuing professional education hours.

GEHA Response:
GEHA recognizes the need to ensure that appropriate education and training opportunities are provided to ensure that technical staff sustain knowledge and skillset in accordance with job responsibilities. Management works with staff to define annual training plans as part of employee performance reviews and department budgets include funding for identified training and/or certification courses.

On October 1, 2018 GEHA is implementing the [redacted] platform. The [redacted] platform includes a learning and development module that will be utilized to track and maintain individual training, certification and continuing professional education (CPE) status.

Management will define and implement a [redacted] to specify requirements and expectations for routine technical training tailored to any position that has privileged or specialized IT, security and/or operational responsibilities as part of their job role.

The estimated completion date is end of Q4 2018.

Network Security – [redacted]
OIG Finding:
GEHA does not have controls in place to [redacted]

Recommendation 4:
We recommend that GEHA implement [redacted].

GEHA Response:
GEHA acknowledges and agrees with the recommendation and [redacted]

Although GEHA is committed to improving our [redacted] as noted above, GEHA has [redacted]

The estimated implementation date for [redacted]

Network Security – Documented Firewall Policy & [redacted]
OIG Finding:
GEHA has firewalls [redacted]. However, GEHA has not formally documented a policy [redacted] Maintaining an approved firewall policy would enable GEH [redacted]

Recommendation 5:
We recommend that GEHA document and approve a firewall policy and/or [redacted]

GEHA Response:
GEHA agrees with the recommendation and is in the process of documenting our firewall [redacted]. Management has [redacted] to perform an [redacted] assessment of all firewall configurations as well as [redacted]

The estimated completion date is the end of [redacted]

Recommendation 6:
We recommend that GEHA perform routine audits of its [redacted]. Note - this recommendation cannot be implemented until the controls from the preceding Recommendation 5 are in place.

GEHA Response:
GEHA agrees with this recommendation. Management has [redacted] aligned with industry best practice and GEHA's security control framework.

Management will establish a process to ensure that regular audits are conducted to ensure compliance with documented configuration standards.

The estimated completion date is the end of [redacted].

Network Security – [redacted]
OIG Finding:
GEHA has implemented [redacted] However, there are [redacted]

Recommendation 7:
We recommend that GEHA implement [redacted].

GEHA Response:
Although [redacted], GEHA acknowledges and agrees with the recommendation and is working to define and implement a network security roadmap that will include the follow key initiatives:

A. Core Upgrade: Establishing the foundation to successfully implement [redacted]
B. Enhanced [redacted] Design: Leverage [redacted]
C. Management Zone: Segregate [redacted]
D. [redacted]

The estimated completion date is the end of Q[redacted]

Configuration Management – Configuration Management Policies
OIG Finding:
GEHA has a configuration management policy requiring its endpoints be securely configured. However, the policy was [redacted]. An updated version of the policy is in progress but has not been approved.

Recommendation 8:
We recommend that GEHA update and approve its corporate configuration management policies.

GEHA Response:
GEHA agrees with this recommendation. Management will review and update the configuration management policies.

The estimated completion date is [redacted]

Configuration Management – [redacted]
OIG Finding:
[redacted]
GEHA has the ability to perform [redacted] on its systems using [redacted]
[redacted]

Recommendation 9:
[redacted]

GEHA Response:
GEHA agrees with this recommendation. [redacted]
[redacted]

The estimated completion date is [redacted]

Recommendation 10:
We recommend that GEHA [redacted]. Note - this recommendation cannot be implemented until the controls from the preceding Recommendation 9 are in place.

GEHA Response:
GEHA agrees with this recommendation. Management will leverage implemented technical solutions (i.e., [redacted] to scan the GEHA technical environment to confirm compliance with approved security configuration standards.

GEHA's environment is scanned [redacted] using the [redacted] vulnerability scanner. Issues and vulnerabilities identified are escalated to the [redacted] and are remediated according to GEHA's [redacted] policy. The [redacted] meets weekly to discuss vulnerability issues, configuration issues and patch compliance status.

GEHA will develop and implement an audit program [redacted]

Configuration Management – Vulnerability Management
OIG Finding:
GEHA routinely conducts [redacted] scans on all servers in its network environment. However, [redacted]

Recommendation 11:
We recommend that GEHA review its patch management policies and procedures and [redacted]

GEHA Response:
GEHA partially agrees with this recommendation. Management has implemented a policy and process to [redacted] to all [redacted] and [redacted] (e.g., [redacted]) through a [redacted] In addition GEHA's environment is scanned [redacted] using the [redacted]. Issues and vulnerabilities identified are escalated to the [redacted]) and are remediated according to GEHA's [redacted] t policy. The [redacted] to discuss vulnerability issues and patch compliance status.

Management recognizes that the [redacted] platforms are currently patched through [redacted] and will work to update current policy and process to ensure these systems are updated on a regular patch schedule.

The estimated completion date is the end of [redacted]

Configuration Management –Unsupported Software
OIG Finding:
[redacted] The vendors of these products typically publicize information [redacted] Having unsupported software leaves GEHA systems vulnerable to infiltration attempts.

Recommendation 12:
We recommend that GEHA upgrade [redacted].

GEHA Response:
GEHA agrees with this recommendation. Management will ensure that the inventory and necessary remediation steps [redacted]

The estimated completion date is the end of [redacted]

Claims Adjudication – Claims Processing System – Paper Claims Tracking & Storage
OIG Finding:
During our walk-through of the claims processing workflow we noted two issues with incoming paper claims. First, GEHA does not have a process to verify that every claim received in the mailroom is scanned and input into the claims processing system.
Second, paper claims are currently stored in a room [redacted] While there are some employee positions that require access to this information, not everyone in the same open area needs access to this sensitive information and there are no physical controls to separate the two areas.

Recommendation 13:
We recommend that GEHA verify that the new contractor has controls to ensure that all incoming claims are properly input for processing and that physical storage of the paper claims implements least privilege.

GEHA Response:
GEHA uses a third party vendor for all paper claims, intake and storage. The vendor [redacted]

[redacted]

We appreciate the opportunity to respond to the draft report.

Sincerely,

Darren Taylor
Chief Operating Officer

Attachments

cc:
[redacted], Program Manager and Contracting Officer, Health Insurance 2
[redacted], Health Insurance Specialist – Contracts
Julie Browne, President & CEO
[redacted], SVP, Health Plan Business Operations

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