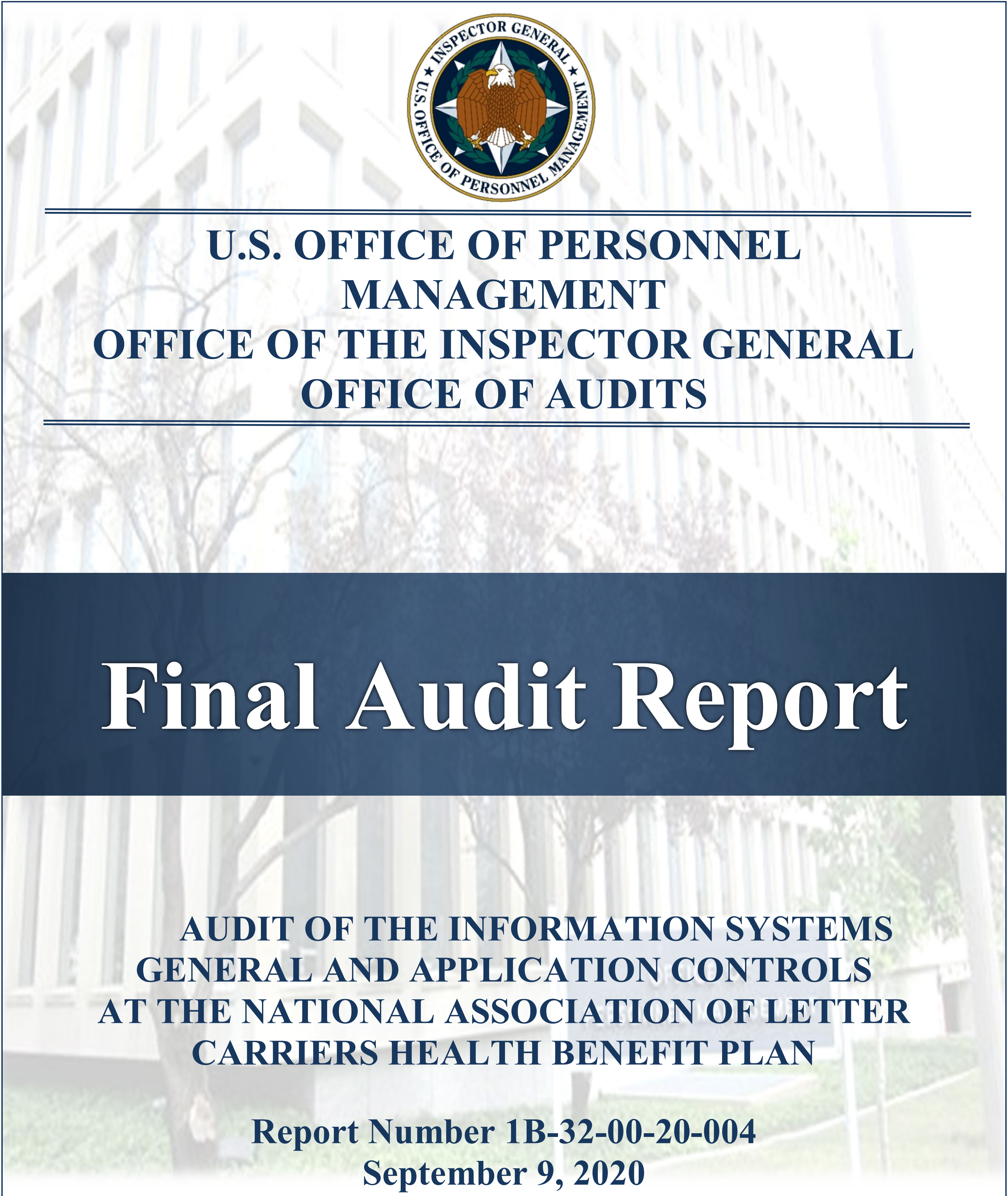

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT THE NATIONAL ASSOCIATION OF LETTER CARRIERS HEALTH BENEFIT PLAN

Report Number 1B-32-00-20-004
September 9, 2020

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at the National Association of Letter Carriers Health Benefit Plan

Report No. 1B-32-00-20-004 **September 9, 2020**

Why Did We Conduct The Audit?

The National Association of Letter Carriers Health Benefit Plan (NALC HBP) 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 NALC HBP's information technology (IT) environment.

What Did We Audit?

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

- NALC HBP does not have an adequate [redacted] process. Furthermore, formal [redacted] are not conducted.
- NALC HBP does not have adequate controls in place related to [redacted]
- NALC HBP does not have adequate controls in place related to [redacted]
- NALC HBP does not have [redacted] Furthermore, NALC HBP's network environment [redacted]
- NALC HBP has documented disaster recovery and business continuity plans. [redacted]
- NALC HBP has a documented application change control process. However, NALC HBP's application change control process [redacted]. Also, NALC HPB does [redacted].

ABBREVIATIONS

CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information Systems Controls Audit Manual
GAO	U.S. Government Accountability Office
IT	Information Technology
NALC HBP	National Association of Letter Carriers Health Benefit Plan
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management

TABLE OF CONTENTS

Page

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 NALC HBP.

The audit was conducted pursuant to FEHBP contract CS 1067; 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, or comprehensive medical services.

This was our third audit of general and application controls at NALC HBP. The previous audits of general and application controls at NALC HBP were conducted in 2004 and 2013. Final Audit Report No. 1B-32-00-04-060 was issued on April 26, 2006, and Final Audit Report No. 1B-32-00-13-037 was issued on May 6, 2014. All recommendations from the previous audits have been closed.

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 NALC HBP's IT environment. We accomplished these objectives by reviewing the following areas:

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

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 NALC HBP'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 NALC HBP'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 NALC HBP to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Ashburn, Virginia.

The onsite portion of this audit was performed in October and November of 2019. 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 NALC HBP as of November 2019.

In conducting our audit, we relied to varying degrees on computer-generated data provided by NALC HBP. 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 NALC HBP'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 NALC HBP'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 NALC HBP's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;

- National Institute of Standards and Technology Special Publication (NIST SP) 800-39, Managing Information Security Risk;

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

- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy; and

- NIST SP 800-160, Volume 1, Systems Security Engineering.

COMPLIANCE WITH LAWS AND REGULATIONS

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

[redacted]

NALC HBP has developed adequate IT security policies and procedures. NALC HBP also has implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

However, we noted the following opportunities for improvement related to NALC HBP's security management program.

1. Risk Management

NALC HBP has implemented adequate policies that govern its risk management program. NALC HBP also has an established Risk Management Committee comprised of a variety of organizational stakeholders that meets quarterly to discuss a wide range of organizational risk. [redacted]

In response to the finding discussed above, NALC HBP provided an updated risk assessment that includes many more identified areas of IT security risk. Conducting a more thorough risk assessment is a positive step in addressing IT security risk. [redacted]

NIST SP 800-39, states that "Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, … resulting from the operation and use of information systems."

[redacted]

Recommendation 1

We recommend that NALC HPB [redacted].

NALC HBP's Response:

"The NALC Health Benefit Plan has revised our Risk Management Plan to reflect FIPS 199 Security Categories. [redacted]

OIG Comment:

In response to the draft audit report, NALC HBP provided evidence demonstrating that detailed milestones with dates [redacted] It appears that NALC HBP's risk response planning has been adequately improved and documented. No further action is required.

2. **Vendor Risk Assessments**

NALC HBP contracts with several vendors that perform business processes related to health claims processing. [redacted]

NIST SP 800-53, Revision 4, advises that [redacted]

[redacted]

Recommendation 2

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan was already tracking Risk Management [redacted]

OIG Comment:

In response to the draft audit report, NALC HBP provided evidence that documentation such as Statement on Standards for Attestation Engagements No. 16 and other independent audit reports related [redacted] Receiving and maintaining this type of independent audit documentation from vendors is a positive step in the right direction. [redacted]

[redacted] to [redacted] prior to [redacted] and then periodically over the course of [redacted]

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 NALC HBP's facilities and data center. We also examined the logical access controls protecting sensitive data on NALC HBP's network environment and claims processing applications.

NALC HBP has adequate physical access controls. [redacted]

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

- Procedures for appropriately granting and removing physical access to facilities and data centers; and
- Procedures for appropriately granting and removing logical access to applications and software resources.

However, we noted the following opportunities for improvement related to NALC HBP's [redacted]

1. Server Administrator Accounts

[redacted]

NIST SP 800-53, Revision 4, advises that [redacted]

[redacted]

Recommendation 3

We recommend that NALC HBP [redacted]

NALC HBP's Response:

The NALC Health Benefit Plan has [redacted]

OIG Comment:

In response to the draft audit report, NALC HBP provided evidence demonstrating that [redacted]. The evidence provided appears to address this recommendation. No further action is required.

2. Privileged User Authentication

NALC HBP does not require [redacted] information systems. [redacted]

NIST SP 800-53, Revision 4, advises that [redacted]

[redacted]

Recommendation 4

We recommend that NALC HBP implement [redacted] on its information systems. Note – this recommendation cannot be implemented until the controls from Recommendation 3 are in place.

NALC HBP's Response:

"The NALC Health Benefit Plan has begun to implement [redacted] ***using a variety of solutions."***

OIG Comment:

In response to the draft audit report, NALC HBP provided a work plan containing detailed milestones with anticipated dates of completion. [redacted]

3. Remote Access

Remote access to NALC HBP's information systems is granted via a virtual private network. [redacted]

NIST SP 800-53, Revision 4, advises that [redacted] Failure to implement [redacted] for remote access to information systems increases the risk that a [redacted] could be compromised and lead to unauthorized access to sensitive data.

<u>Recommendation 5</u>

We recommend that NALC HBP implement [redacted] to access systems remotely.

<u>NALC HBP’s Response:</u>

“The NALC Health Benefit Plan has begun to implement [redacted] using a variety of solutions.”

4. <u>Shared Administrator Account Management</u>

We conducted logical access testing and identified a large number of [redacted] on NALC HBP systems. NALC HBP’s [redacted] ” has a section related to [redacted] and states that [redacted], except under special circumstances, where [redacted] may be used. NALC HBP does not appear to be following this policy, as [redacted] In response to this finding, NALC HBP has provided an updated risk assessment that includes evaluating the necessity of existing [redacted]

NIST SP 800-53, Revision 4, advises that [redacted]

Furthermore, NIST SP 800-53, Revision 4, advises that “[redacted]” Failure to properly manage the [redacted] increases the risk that malicious activity cannot be [redacted].

Recommendation 6

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan has reviewed the list of [redacted] ***Explanations have been provided for*** [redacted]

OIG Comment:

In response to the draft audit report, NALC HBP provided evidence demonstrating that [redacted] are currently being reviewed and some [redacted]. However, based on the evidence provided it appears that [redacted] are still under review in order to verify if [redacted] As a part of the audit resolution process, please provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence that NALC HBP has fully implemented this recommendation.

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.

[redacted]

We evaluated NALC HBP's network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public network connections;
- Web content filtering to protect against malicious websites; and
- Documented policies and procedures to audit firewall changes.

However, we noted the following opportunities for improvement related to NALC HBP's network security controls.

1. Firewall Policy

NALC HBP maintains high level firewall management guidance within its "Network Security Management Policy." The policy states that standard firewall configurations must be approved. However, NALC HBP does not have a firewall policy that documents approved firewall configurations. NIST SP 800-41, Revision 1, identifies key elements or details of a firewall policy including:

- [redacted]; and
- Guidance on performing risk assessments to create '[redacted]

NIST SP 800-41, Revision 1, also states that a[redacted]

[redacted]

Recommendation 7

We recommend that NALC HBP [redacted].

NALC HBP's Response:

"The NALC Health Benefit Plan has developed a plan to address this recommendation."

2. Internal Network Segmentation

NALC HBP uses firewalls to control connections with systems outside of its network as well as between public-facing applications and the internal network. [redacted]

NALC HBP [redacted]

NIST SP 800-41, Revision 1, advises that, "[redacted]

Failure to appropriately [redacted] from [redacted]

Recommendation 8

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan continues to make progress [redacted] ***"***

3. Network Access Control

NALC HBP's "Network Security Management Policy" states that only authorized computers will be able to access the internal network. [redacted]

NIST SP 800-53, Revision 4, states that an information system should uniquely identify and authenticate devices before establishing a network connection.

[redacted]

Recommendation 9

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan continues* [redacted]*"

4. Vulnerability Scanning

NALC HBP's "Malicious Software Management Policy" states that network vulnerability scans are performed at least bi-weekly. Per policy, NALC HBP performs routine credentialed vulnerability scans on workstations. [redacted]

NIST SP 800-53, Revision 4, advises that the organization "Scans for vulnerabilities in the information system and hosted applications" and "Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk."

Furthermore, NIST SP 800-53, Revision 4, states that the organization should implement privileged access authorization for vulnerability scanning activities.

[redacted]

Recommendation 10

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan continues to make progress on Vulnerability Scanning."

OIG Comment:

In response to the draft audit report, NALC HBP provided work plans related to developing security configuration standards and automated patch management procedures. The work plan milestones do describe scanning initial workstation and server builds for vulnerabilities. [redacted]

[redacted]

5. Vulnerabilities Identified by OIG Scans

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers, workstations, and a public facing web application in NALC HBP's network environment. The specific vulnerabilities that we identified were provided to NALC HBP in the form of an audit inquiry, but will not be detailed in this report. NALC HBP was [redacted]. However, [redacted] the issues we found.

NIST SP 800-53, Revision 4, states that organizations should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

[redacted]

Recommendation 11

We recommend that NALC HBP [redacted] discovered during this audit as outlined in the [redacted] audit inquiry.

NALC HBP's Response:

"The NALC Health Benefit Plan continues to make progress** [redacted] **during the Audit."

6. Network Monitoring

NALC HBP utilizes tools at its network perimeter to monitor network traffic. Furthermore, NALC HBP contracts with a vendor to collect, aggregate, and monitor suspicious log activity. [redacted]

[redacted]

NIST SP 800-53, Revision 4, states that organizations should routinely review and analyze information system audit records for indications of inappropriate or unusual activity.

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

[redacted]

<u>Recommendation 12</u>

We recommend that NALC HPB [redacted]

<u>NALC HBP's Response:</u>

"The NALC Health Benefit Plan recently received approval from its governing body to implement a new [redacted]

7. <u>Incident Response Testing</u>

NALC HBP has a documented and approved "Cyber Incident Response Plan." The plan requires testing and training for employees responsible for responding to incidents. [redacted]

In response to the finding discussed above, NALC HBP performed an incident response test that included key members of the organization. In addition to the test results, NALC HBP provided "[redacted]" used to evaluate the exercise and an updated "Cyber Incident Response Plan."

As a result of NALC HBP conducting an incident response test before the issuance of the draft audit report, we will not issue a recommendation. However, we encourage NALC HBP to continue performing routine incident response tests in the future. Regular test results should be used to improve the "Cyber Incident Response Plan."

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

Our review found the following controls in place:

- A documented system change control process; and

- An established patch management process.

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

1. Security Configuration Standards

Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers. [redacted]

[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.

[redacted]

Recommendation 13

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan [redacted]***."***

2. Security Configuration Auditing

As noted above, [redacted]

NIST SP 800-53, Revision 4, [redacted]

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.

[redacted]

Recommendation 14

We recommend that NALC HBP implement a process [redacted] Note – this recommendation cannot be implemented until the controls from Recommendation 13 are in place.

NALC HBP's Response:

"The NALC Health Benefit Plan has developed a plan to address this recommendation."

OIG Comment:

In response to the draft audit report, NALC HBP provided work plans related to hardening servers and workstations and developing an automated patching process. The work plans appear to be adequate for developing security configuration standards, which apply to Recommendation 13. [redacted]

3. System Lifecycle Management

NALC HBP [redacted] NALC HBP's [redacted] NALC HBP's [redacted]

NIST SP 800-53, Revision 4, [redacted] NIST SP 800-53, Revision 4, [redacted]

[redacted]

Recommendation 15

We recommend that NALC HBP implement policies and procedures [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan [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 NALC HBP's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

[redacted]

- Data center environmental controls to minimize disruptions;
- Business continuity plan (e.g., people and business processes); and
- Disaster recovery plan (e.g., recovery of hardware and software infrastructure).

However, we noted the following opportunities for improvement related to NALC HBP's contingency planning.

1. Business Continuity Plan Testing

NALC HBP's business continuity plan includes an alternate facility at which personnel can continue business operations, such as claims processing, in the event the primary location becomes unavailable. [redacted]

NIST SP 800-53, Revision 4, advises that ‘[redacted]

[redacted]

Recommendation 16

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan has [redacted] ***through the current Pandemic crisis."***

OIG Comment:

In response to the draft audit report, NALC HBP provided a document stating that the Business Continuity Plan has been enacted due to the COVID-19 crisis and as such, a majority of its employees have been successfully teleworking since March, 24 2020. [redacted]

2. Disaster Recovery Plan Testing

NALC HBP's disaster recovery plan includes a detailed process to recover critical IT infrastructure and applications at an alternate location. [redacted]

NIST SP 800-53, Revision 4, advises that, "The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing."

[redacted] NALC HBP [redacted]

Recommendation 17

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan [redacted]

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting NALC HBP's claims adjudication process. NALC HBP adjudicates claims using an internally developed claims processing application called [redacted] We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment and suspension.

1. Application Change Control

We evaluated the policies and procedures governing application development and change control over NALC HBP's claims processing system.

NALC HBP has implemented policies and procedures related to application configuration management, and has adopted a system development life cycle methodology that IT personnel follow during routine software modifications. However, we noted the following opportunities for improvement related to NALC HBP's application change control process.

Security Roles and Responsibilities

NALC HBP's "System Development Lifecycle Policy" states that levels of security are required to protect NALC HBP's information. [redacted] NALC HBP's "System Development Lifecycle Policy" [redacted]

NIST SP 800-160, Volume 1, states that '[redacted]

[redacted]

Recommendation 18

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan revised [redacted]

OIG Comment:

In response to the draft audit report, NALC HBP provided an updated "System Development Lifecycle Policy" draft that defines security roles and responsibilities related to system changes. [redacted]

SDLC Compliance Reviews

NALC HBP [redacted]

NIST SP 800-53, Revision 4, advises that the organization "Audits and reviews activities associated with configuration-controlled changes to the information system … ."

Recommendation 19

We recommend that NALC HBP [redacted]

NALC HBP's Response:

"The NALC Health Benefit Plan revised our [redacted]

OIG Comment:

In response to the draft audit report, NALC HBP provided an updated "System Development Lifecycle Policy" draft that identifies a process to review changes after completion. [redacted]

2. Claims Processing System

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

NALC HBP has sufficient input, processing, and output controls over claims processing.

- Claims are properly input and tracked to ensure timely processing;
- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and
- Claims scheduled for payment are actually paid.

Nothing came to our attention to indicate that NALC HBP has not implemented adequate controls over the claims processing system.

3. Enrollment

We evaluated NALC HBP's procedures for managing its member enrollments. 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 NALC HBP has not implemented adequate controls over the enrollment process.

4. Debarment and Suspension

NALC HBP has documented procedures for reviewing provider files for debarments and suspensions. NALC HBP downloads the OPM OIG debarment and suspension list and performs a comparison with provider records and claims history maintained in [redacted] Positive matches from the list are identified within [redacted] and a notification letter is sent to members. If a debarred or suspended provider submits a claim, the claims processing application will suspend the claim for review by a claims processor. NALC HBP adheres to the OPM OIG debarment and suspension guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

Nothing came to our attention to indicate that NALC HBP has not implemented adequate controls over the debarment and suspension process.

APPENDIX

NATIONAL ASSOCIATION OF LETTER CARRIERS
HEALTH BENEFIT PLAN
20547 Waverly Court, Ashburn, Virginia 20149 ● (703)729-4677 or 888-636-NALC (6252)
Fredric V. Rolando, President ● **Stephanie M. Stewart,** Director

June 8, 2020

[redacted], Auditor-in-Charge
Information Systems Audit Group
U.S. Office of Personnel Management
Office of the Inspector General

Reference: OPM Draft Audit Report – Information Systems General and Application Controls
National Association of Letter Carriers Health Benefit Plan (NALC HBP or Plan)
Audit Report No: 1B-32-00-20-004

The following represents NALC HBP's response to the recommendations included in the draft report.

A. SECURITY MANAGEMENT

1. Risk Management

Recommendation 1
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan has revised our Risk Management Plan to reflect FIPS 199 Security Categories. [redacted]

2. Vendor Risk Assessments

Recommendation 2
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan was already tracking Risk Management [redacted]. See Exhibit 1-A Vendor RM.

B. ACCESS CONTROLS

1. Vendor Risk Assessments

Recommendation 3
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan has [redacted]

2. Privileged User Authentication

Recommendation 4
We recommend that NALC HBP implement [redacted] Note – this recommendation cannot be implemented until the controls from Recommendation 3 are in place.

Plan Response
The NALC Health Benefit Plan has begun to implement [redacted] using a variety of solutions. See Exhibit 1-B [redacted]/Risk Plan.

3. Remote Access

Recommendation 5
We recommend that NALC HBP implement [redacted] to access systems remotely.

Plan Response
The NALC Health Benefit Plan has begun to implement [redacted] using a variety of solutions. See Exhibit 1-B [redacted] Risk Plan.

4. Shared Administrator Account Management

Recommendation 6
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan has reviewed the list of [redacted] Explanations have been provided [redacted] See Exhibit 3.

C. NETWORK SECURITY

1. Firewall Policy

Recommendation 7
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan has developed a plan to address this recommendation. See Exhibit 1-C [redacted]Risk Plan.

2. Internal Network Segmentation

Recommendation 8
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan continues to make progress [redacted] See Exhibit 1-D Network Segmentation Project/Risk Plan.

3. Network Access Control

Recommendation 9
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan continues to make progress [redacted] See Exhibit 1-D [redacted] Risk Plan.

4. **Vulnerability Scanning**

Recommendation 10
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan continues to make progress [redacted] See Exhibit 1-E [redacted] Risk Plan & 1-F [redacted] Risk Plan.

5. **Vulnerabilities Identified by OIG Scans**

Recommendation 11
We recommend that NALC HBP [redacted] during this audit as outlined in the [redacted] audit inquiry.

Plan Response
The NALC Health Benefit Plan continues to make progress [redacted] during the Audit. See Exhibit 1-F [redacted] Risk Plan and Exhibit 1-G [redacted]

6. **Network Monitoring**

Recommendation 12
We recommend that NALC HPB [redacted]

Plan Response
The NALC Health Benefit Plan recently received approval from its governing body to implement a new [redacted]

D. CONFIGURATION MANAGEMENT

1. Security Configuration Standards

Recommendation 13

We recommend that NALC HBP [redacted]

Plan Response

The NALC Health Benefit Plan has developed a plan to address this recommendation. See Exhibit 1-E [redacted] Risk Plan [redacted] Risk Plan.

2. Security Configuration Auditing

Recommendation 14

We recommend that NALC HBP implement a process to [redacted] Note – this recommendation cannot be implemented until the controls from Recommendation 13 are in place.

Plan Response

The NALC Health Benefit Plan has developed a plan to address this recommendation. See Exhibit 1-E [redacted] Risk Plan & [redacted] Risk Plan.

3. System Lifecycle Management

Recommendation 15

We recommend that NALC HBP implement policies and procedures [redacted]

Plan Response

The NALC Health Benefit Plan [redacted] See Exhibit 1-G [redacted] Risk Plan.

E. CONTINGENCY PLANNING

1. Business Continuity Plan Testing

Recommendation 16
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan [redacted] through the current Pandemic crisis. See Exhibit 4 – Testing 2020 and COVID-19 Actions Taken.

2. Disaster Recovery Plan Testing

Recommendation 17
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan [redacted] See Exhibit 1-H [redacted]

F. CLAIMS ADJUDICATION

1. Application Change Control

Recommendation 18
We recommend that NALC HBP [redacted]

Plan Response
The NALC Health Benefit Plan revised [redacted]

Recommendation 19
We recommend that NALC HBP [redacted]

Plan Response

The NALC Health Benefit Plan revised our [redacted] [redacted] See Exhibit 5 – IS-30 [redacted]

Sincerely,

[redacted]

Stephanie M. Stewart
Director
National Association of Letter Carriers Health Benefit Plan

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