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

Final Audit Report

Subject:

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

Report No. 1B-32-00-13-037

Date: May 6, 2014

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1067
NATIONAL ASSOCIATION OF LETTER CARRIERS
HEALTH BENEFIT PLAN
PLAN CODE 32
ASHBURN, VIRGINIA

Report No. 1B-32-00-13-037

Date: May 6, 2014

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1067
NATIONAL ASSOCIATION OF LETTER CARRIERS
HEALTH BENEFIT PLAN
PLAN CODE 32
ASHBURN, VIRGINIA

Report No. 1B-32-00-13-037

Date: May 6, 2014

This final report discusses the results of our audit of general and application controls over the information systems at the National Association of Letter Carriers Health Benefit Plan (NALC HBP or Plan).

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for NALC HBP, as well as the various processes and information technology (IT) systems used to support these applications. We documented controls in place and opportunities for improvement in each of the areas below.

Security Management

NALC HBP has not developed an adequate security management program. NALC HBP has not developed IT security policies and procedures, implemented a formal security awareness training program or a specialized training program, and has not established a formal risk management program.

Access Controls

NALC HBP has not implemented adequate physical access controls surrounding its facilities and data center. Additionally, we documented several opportunities for improvement related to

NALC HBP's logical access controls related to password policy, segregation of duties, and monitoring user accounts.

Network Security

Our review of the network security controls indicated that the NALC HBP has implemented and utilizes a firewall to protect its network environment. However, we noted several areas of concern:

- Formal policies and procedures have not been implemented for:
  - Security Incident Response,
  - Vulnerability Management and Remediation,
  - Patch Management, and
  - Firewall Configuration Management;
- Vulnerability scan results indicate that critical patches, service packs, and hot fixes are not implemented in a timely manner; and
- The Plan does not have controls to detect and prevent unauthorized devices from connecting to the internal network.

Configuration Management

NALC HBP has not developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured and updated. NALC HBP has not documented formal baseline configurations for all of the utilized operating platforms and, as a result, is unable to routinely audit its network servers' configuration to any approved configuration settings. NALC HBP has also not established a formal systems development lifecycle methodology. NALC HBP has documented corporate password standards, but we discovered many instances where information systems did not follow the established guidelines.

Contingency Planning

NALC HBP has not conducted an adequate business impact analysis. Currently, NALC HBP does not have an alternate location to recover its computing environment in the event of a disaster at its primary data center. NALC HBP has also not established an alternate work site for its employees to allow for critical business operations to continue if the main facility is not accessible. The backup power generator at the NALC HBP facility does not have the capacity to sustain the data center in the event of a prolonged power outage. NALC HBP's contingency plan does not address many of the suggested elements of relevant guidance, and the plan is not tested routinely. NALC HBP also does not routinely perform emergency response training related to business continuity and disaster recovery for its employees with responsibilities in these areas.

Claims Adjudication

NALC HBP has implemented many controls in its claims process to ensure that FEHBP claims are processed accurately with regard to enrollment and debarment. However, we noted significant weaknesses [redacted] NALC HBP informed the OIG that Cigna, its pricing vendor, may have edits in place to prevent or identify these issues, but to date has not provided sufficient evidence to support this

claim. As a result, we are issuing this report with the assumption that no additional controls exist.

Health Insurance Portability and Accountability Act (HIPAA)

The Plan developed a series of privacy policies and procedures that address requirements of the HIPAA privacy rule. However, not all of the elements of the HIPAA security rule have been implemented.

Contents

I. Introduction

This final report details the findings, conclusions, and recommendations resulting from our audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) claims by the National Association of Letter Carriers Health Benefit Plan (NALC HBP or Plan).

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.

Background

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

This was our second audit of NALC HBP's general and application controls. The first audit was conducted in 2004 and all recommendations from that audit were closed prior to the start of the current audit. We also reviewed NALC HBP's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

During the field work phase of this audit, we issued a flash audit alert to bring immediate attention to serious concerns we had regarding NALC HBP's ability to adequately secure sensitive Federal data. The alert included two recommendations that we believed were urgent in nature, and advised NALC HBP to begin immediately taking steps to address the weaknesses.

All NALC HBP personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated. We would also like to commend the Plan for taking prompt corrective actions on many of the recommendations within this report.

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;
- Configuration management;
- Segregation of duties;

- Contingency planning;
- Application controls specific to NALC HBP's claims processing system; and
- HIPAA compliance.

Scope

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 for FEHBP members, with a primary focus on the claims adjudication applications. NALC HBP claims are priced through a third party, Cigna, before they are processed by [redacted] the Plan's claims adjudication system. The business processes reviewed are primarily located in NALC HBP's Ashburn, Virginia facility.

The on-site portion of this audit was performed from June through July of 2013. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at NALC HBP as of August 2013.

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.

Methodology

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed NALC HBP's business structure and environment;
- Performed a risk assessment of NALC HBP's information systems environment and applications, and prepared an audit program based on the assessment and the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

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

- Title 48 of the Code of Federal Regulations;
- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-61, Computer Security Incident Handling Guide;
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule; and
- HIPAA Act of 1996.

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 the "Audit Findings and Recommendations" section of this report.

II. Audit Findings and Recommendations

A. Security Management

The security management component of this audit involved the examination of the policies and procedures that are the foundation of NALC HBP's overall IT security controls. 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. We also reviewed NALC HBP's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

The sections below outline our concerns with NALC HBP's security management program.

1. Entity-Wide IT Policies and Procedures

NALC HBP has not developed comprehensive IT security policies and procedures. IT policies and procedures are the critical foundation of a strong information security program, as these documents provide guidance on how IT security should be managed at a specific organization.

FISCAM states that "Entities should have a written plan that clearly describes the entity's security program, and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources. . . . To be effective, the policies and plan should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use."

Without well-defined IT security policies, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied.

Recommendation 1 (from Flash Audit Alert issued July 29, 2013)

We recommend that NALC HBP develop comprehensive IT security policies and procedures. At a minimum, NALC HBP should implement policies and procedures related to the following topics:

- Risk Assessments
- Contingency Planning and Testing
- Security Awareness Training
- Employee Termination
- Physical Access Controls
- Auditing/Monitoring User and Administrator Activity
- Appropriate Use of Software
- Password Requirements
- Vulnerability Scanning
- Server Configuration Management, Baseline Configurations, and Auditing Server Configuration
- System Development Lifecycle
- Firewall Management
- Web and E-mail Filtering

- Segregation of Duties
- Security Incident Response
- Wireless Network Access
- Control of Removable Media

NALC HBP Response:

"The NALC HBP has developed and adopted the attached Information Security Policies and Procedures"

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has developed detailed policies and procedures for its IT security program; no further action is required.

Recommendation 2

We recommend that NALC HBP implement a process to routinely review and update its IT security policies.

NALC HBP Response:

"The NALC HBP has established an Information Security Management Committee.

The committee members are: NALC HBP Director, the NALC HBP Administrator, the Human Resources Manager, the Facilities Manager, the Information Systems Manager, the Claims Superintendent, the HIPAA Security Officer and the HIPAA Privacy Official.

The committee, in conjunction with members of the Information Systems Department staff and representatives from the Administrative and Claims departments, have been integral in formulating the newly established policies. The committee will meet annually prior to the scheduled risk assessment to review and update IT security policies.

Policies will be addressed accordingly if circumstances dictate a review and update prior to the scheduled event.

The NALC HBP policy is now formally documented in IS-01 Information Security Program Policy on Policies and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process to routinely review and update its IT security policies; no further action is required.

2. Security Awareness Training

NALC HBP has not implemented a formal security awareness training program for its full-time, part-time, temporary, or contractor employees.

Section 164.308(5)(i) of HIPAA states that the organization must, "Implement a security awareness and training program for all members of its workforce (including management)."

Without a formal security awareness training program, employees cannot be held accountable for security breaches, as they have not been properly trained. Without regular awareness training, employees may not be aware of their responsibilities for protecting the organization's resources. This lack of employee knowledge and understanding could expose NALC HBP's confidential information to unauthorized personnel.

Recommendation 3

We recommend that as part of its efforts to obtain compliance with the HIPAA security rule, NALC HBP implement a security awareness training program for its employees. For guidance in creating a security awareness program see NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

NALC HBP Response:

"The NALC HBP is in the process of creating a security awareness program based upon our own policies in conjunction with outside resources. Specifically we have contacted [redacted] regarding their – [redacted] educational suite and [redacted] regarding their [redacted] product. Upon selection of the appropriate product, we will incorporate pertinent materials into our security program.

We are anticipating an April 2014 launch for our security awareness training program for all employees and will update our new employee educational material to address the security requirements."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's Healthcare and Insurance Office (HIO) with supporting evidence when a security awareness training program has been developed and implemented.

3. Specialized Training

Personnel responsible for the administrative, technical, and operational security of NALC HBP's technical operating environment do not receive the routine training necessary to adequately monitor and maintain the Plan's network infrastructure and external access points to its information system resources.

According to NIST SP 800-12 Chapter 13, "Many groups need more advanced or more specialized training than just basic security practices. For example, managers may need to understand security consequences and costs so they can factor security into their decisions, or system administrators may need to know how to implement and use specific access control products. . . . A security training program normally includes training classes, either strictly devoted to security or as added special section or modules within existing training classes.

Training may be computer- or lecture-based (or both), and may include hands-on practice and case studies."

Without a specialized training program, the personnel responsible for IT security at NALC HBP are not equipped with the necessary knowledge to identify and address security weaknesses, implement and use access control and system monitoring tools, or understand the security consequences and costs that should be factored into their decisions.

Recommendation 4

We recommend that NALC HBP develop and implement a training program for employees with IT security responsibilities. The program should include:

- A process to identify and categorize positions with security responsibilities;
- Inclusion of specialized security training requirements within job descriptions;
- Opportunities to seek and maintain technical certifications;
- Documentation of training completed by each employee; and
- A periodic review of employee records to ensure that specialized security training is completed in accordance with standards.

NALC HBP Response:

"The NALC HBP is reviewing outside sources for purposes of establishing specialized training for employees with IT security responsibilities, which will include the bulleted items above. The sources contacted to date are [redacted].

The NALC HBP has always encouraged and has a documented history of allowing our employees opportunities to seek and maintain technical certifications."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence when a training program for employees with elevated IT security responsibilities has been developed and implemented.

4. Risk Assessment

NALC HBP has not established a risk management program that identifies, classifies, and mitigates human or environmental threats to its computer-based operating environment.

According to FISCAM, "Risk assessments should consider data sensitivity and integrity and the range of risks that an entity's systems and data may be subject to, including those posed by authorized internal and external users, as well as unauthorized outsiders who may try to 'break into' the systems."

HIPAA Security and Privacy Standard 164.308(a)(l)(ii), requires organizations to:
"(A). . . Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. . . .

(B). . . Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."

Recommendation 5

We recommend that NALC HBP develop and implement a risk management policy and a risk assessment methodology. NIST SP 800-30 Revision 1 serves as an excellent reference to assist NALC HBP with the development of its risk management program. Implementation of the suggested framework would also help NALC HBP obtain compliance with the HIPAA Security Rule.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-19 IT Risk Management Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has developed and implemented a risk management policy and a risk assessment methodology; no further action is required.

B. Access Controls

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources.

We examined the physical access controls of NALC HBP's facility and data center. We also examined the logical controls protecting sensitive data in NALC HBP's network environment and claims processing related applications.

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

- Procedures for appropriately authorizing physical access to the facility and data center; and
- Procedures for revoking access to the facility and data center for terminated employees.

The following sections document several opportunities for improvement related to NALC HBP's physical and logical access controls.

1. Password policy

NALC HBP does not have policies or procedures for creating, changing, and safeguarding passwords. In addition, the current configuration of password-related values for [redacted] do not provide adequate protection against unauthorized system access.

Section 164.308(5)(ii)(D) of the HIPAA security rule requires an organization to document procedures for creating, changing, and safeguarding passwords; FISCAM provides password guidelines; and NIST SP 800-14 outlines requirements for the creation and maintenance of IDs and passwords.

Failure to implement a strong password policy puts sensitive data at risk to malicious attacks.

Recommendation 6

We recommend that NALC HBP implement a password policy that closely reflects industry standards.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-05 Account Management Policy and will be effective on February 1, 2014. We believe the policy provides appropriate safeguards in light of NALC HBP's business needs."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a password policy that utilizes industry best practices; no further action is required.

Recommendation 7

We recommend that NALC HBP address its [redacted] password setting weaknesses once a standard password policy has been implemented for the organization.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-05 Account Management Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a password policy that utilizes industry best practices. However, as part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence that the [redacted] password settings comply with the Plan's new password policy.

2. Segregation of duties

NALC HBP has three domain administrators that share a single user account for [redacted] This user account is not monitored and audit logs of the account's activity are not reviewed.

FISCAM states that "Work responsibilities should be segregated so that one individual does not control all critical stages of a process."

NIST SP 800-53, Revision 4, states that the organization must separate "duties of individuals as necessary, to prevent malevolent activity without collusion; documents separation of duties; and implements separation of duties through assigned information system access authorizations."

Failure to implement adequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, that improper changes could be implemented, or that computer resources could be damaged or destroyed. With no routine review of privileged user activity, NALC HBP is not able to link users to specific tasks performed. This increases the risk that malicious activity could go undetected and sensitive information could be compromised.

Recommendation 8

We recommend that NALC HBP establish unique user accounts for each privileged user.

NALC HBP Response:

"The NALC HBP has created unique user accounts for privileged users. At present, three Information Systems staff senior managers have unique privileged accounts on the network and on the [redacted] The Network Administrator has a unique privileged account on the network but not on the [redacted] The Programming Staff members have a lesser set of privileges on the [redacted] than the senior managers but no special network privileges. The Operations staff has a unique set of privileges on the [redacted] that are different than the programming staff and lesser than the senior managers and have a unique set of privileges on the network that are lesser than the senior managers.

The NALC HBP policy is now formally documented in IS-04 Access Control Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has established unique user accounts for privileged users; no further action is required.

Recommendation 9

We recommend that NALC HBP implement a process to routinely review privileged user activities.

NALC HBP Response:

"We have contracted with a third-party to provide an appliance and application that will allow them to monitor account activity on our behalf. This will provide real-time alerts based upon the sensitivity settings and will allow immediate review as required. A full review will be conducted weekly by internal and/or the third party sources.

The NALC HBP policy is now formally documented in IS-18 Monitoring and Log Management Policy."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process to routinely review privileged user activities; no further action is required.

3. Monitoring of Active Accounts

NALC HBP does not audit or review [redacted] user accounts. For [redacted] accounts, the database administrator selects a subset of accounts to review, but there is no formal procedure in place outlining what should be looked at during this review. We performed a test to evaluate whether administrators are appropriately removing an employee's logical access after termination. The results indicated that seven [redacted] accounts were not properly removed after the employees' termination.

NALC HBP has no process in place to review the appropriate level of access for active user accounts for any of the applications used to gain access to sensitive data. We could not conduct independent testing for appropriateness because NALC HBP does not document the access level approved for each user.

NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPPA Security Rule, states that organizations should develop "procedures for reviewing and, if appropriate, modifying access authorizations for existing users." Furthermore, NIST SP 800-12, An Introduction to Computer Security, states that access reviews should "examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth."

Recommendation 10

We recommend that NALC HBP implement a process to review logical access to all of its systems and supporting applications to ensure that no terminated individuals retain access.

NALC HBP Response:

"A list of all active employees will be forwarded to the Information Systems Department by the Human Resources department [redacted] The Information Systems Department will compare the list against active network accounts and active [redacted] accounts for accuracy. Accounts will be adjusted accordingly.

Documentation of the review will be retained in the Human Resources Department.

The NALC HBP policy is now formally documented in IS-04 Access Control Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process to review access to all of its systems to ensure that no terminated individuals retain access; no further action is required.

Recommendation 11

We recommend that NALC HBP implement a process to review active user accounts across major applications for appropriateness.

NALC HBP Response:

"The Information Systems Department will conduct [redacted] review of all network accounts for appropriate levels of access. The NALC HBP is assessing a monitoring tool from [redacted] for [redacted] accounts to ensure appropriate levels of access. The Information Systems Department will compare the list against active network accounts and active [redacted] accounts for accuracy. Accounts will be adjusted accordingly.

The NALC HBP policy is now formally documented in IS-04 Access Control Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process review the level of access for active user accounts for all applications containing sensitive data; no further action is required.

4. Weaknesses Identified in Physical Access Controls

Data Center

NALC HBP's data center did not contain several controls that we typically observe at similar facilities, including:

- multi-factor authentication to enter the computer room (e.g., cipher lock or biometric device in addition to an access card);
- piggybacking alarms to enter the computer room (alarm that sounds if more than one person walks past a sensor for each access card that is swiped); and
- video monitoring at the entrances.

The data center contains a cypher lock to control access. [redacted]

Failure to implement proper physical access controls increases the risk that unauthorized individuals can gain access to NALC HBP's data center and the sensitive resources and confidential data it contains.

NIST SP 800-53 Revision 4 provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 12

We recommend that NALC HBP improve the physical access controls at its data center. At a minimum, the computer room should have multi-factor authentication and piggybacking controls at both entrances.

NALC HBP Response:

"The NALC HBP is in agreement and is soliciting proposals from qualified vendors to augment the current physical access controls at its data center to include multi-factor authentication and alarm-based anti-piggyback controls at both entrances."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence when physical access controls at the data center have been improved to include multi-factor authentication and anti-piggybacking controls.

Facility

NALC controls physical access to its facility with proximity card readers, CCTV surveillance and security guards posted inside the building's two main entrances. However, the following elements of NALC HBP's facility security controls could be improved:

- a routine audit of active access cards;
- a recertification process for employees with specialized access to the building;
- the temporary badge termination process; and
- implement piggybacking controls.

We compared a list of employees that were terminated within the last three years to a list of active access cards and discovered that six terminated employees still had access to NALC HBP's facility. In response to this test finding NALC HBP immediately removed the access of the terminated employees.

A limited group of employees, including the Director and senior management, are granted unrestricted access at every entrance to NALC HBP's facility 24 hours a day and 7 days a week. However, there is currently no process in place to recertify that these employees still require this level of access to the facility.

Temporary badges for visitors could be set to expire after a certain pre-determined period of time; however, NALC HBP does not enforce this. When access for a visitor is no longer required, an email is manually sent to the facilities director as a reminder to remove the visitor's access.

In addition, NALC HBP does not have physical access controls in place to prevent employees from piggybacking into secure areas (one person using an electronic access card to open a door, then holding that door open while others enter).

FISCAM states that "Controls should accommodate employees who work at the entity's facilities on an everyday basis; occasional visitors, such as employees of another entity facility or maintenance people; and infrequent or unexpected visitors. Physical controls vary, but include: manual door or cipher key locks, magnetic door locks that require the use of electronic keycards, biometrics authentication, security guards, photo IDs, entry logs, and electronic and visual surveillance systems."

Also, FISCAM states that "By obtaining physical access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software."

In addition, NIST SP 800-53 Revision 4 provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 13

We recommend that NALC HBP implement a process for routinely auditing all active access cards to ensure that they are not assigned to terminated employees.

NALC HBP Response:

"A list of all active access cards will be forwarded by the facilities manager [redacted] to Human Resources to ensure

- ***Cards are issued to active employees only***
- ***Access level is appropriate for duties***
- ***Card number corresponds with ID number***

The review of active access cards will be conducted by the Human Resources Department staff and a log of the event review will be maintained in that department.

The NALC HBP policy is now formally documented in IS-12 Physical Access Security Policy and will be effective on February 1, 2014. These are also reflected in HR Policies and Procedures Manual."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process to routinely audit all active access cards to ensure they are no longer assigned to terminated employees; no further action is required.

Recommendation 14

We recommend that NALC HBP implement a process to routinely recertify that employees with specialized access still require such access. If no specialized access is required, then the access level should be adjusted accordingly.

NALC HBP Response:

"A list of all specialized Access Cards will be forwarded [redacted] to the Administrative Office for review or more frequently as changes become necessary. Upon review, specialized access will be adjusted accordingly.

Documentation of the review will be retained in the Human Resources Department.

The NALC HBP policy is now formally documented in IS-12 Physical Access Security Policy and will be effective on February 1, 2014. These are also reflected in HR Policies and Procedures Manual."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a recertification process to ensure employees with specialized access still require that level of access and when that access is no longer required it is promptly removed; no further action is required.

Recommendation 15

We recommend that NALC HBP implement a process to automatically disable temporary access badges.

NALC HBP Response:

"Temporary cards are activated upon request from Human Resources when an employee forgets their permanent access badge. Our current system is unable to deactivate automatically. An RFI is being solicited for upgrade/replacement of Access System.

In the interim, temporary cards are deactivated manually [redacted].

The NALC HBP policy is now formally documented in IS-12 Physical Access Security Policy and will be effective on February 1, 2014. These are also reflected in HR Policies and Procedures Manual."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence of the upgraded/replacement badging system.

Recommendation 16

We recommend that NALC HBP reassess the physical access controls at its facility and implement controls that will ensure proper physical security. At a minimum, NALC HBP should implement a piggybacking control at the two main entrances to the facility.

NALC HBP Response:

"The NALC HBP acknowledges the concern and has been actively investigating potential solutions to address the piggybacking issue highlighted by the OIG. While similar in nature to the concern raised with respect to the data center controls, we have determined the approach must be different due to the higher volume of employees passing through these entrances, and may involve the use of a turnstile or similar system. Any modification of the two main entrances of this nature must also be fully ADA compliant, will require building owner authorization and the appropriate building code permits."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence once the Plan has implemented an appropriate level of physical access controls at the two main entrances to their facility.

C. Network Security

Network security includes the policies and controls used to prevent or detect unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. NALC HBP has recently begun to implement an incident response and network security program.

We evaluated NALC HBP's network security program and reviewed the results of several automated vulnerability scans we performed during this audit. We noted the following opportunities for improvement related to NALC HBP's network security controls.

1. Incident Response

NALC HBP has not implemented a formal incident response policy or procedure. NALC HBP has recently implemented an intrusion detection system that, if configured appropriately, has the ability to detect certain levels of intrusion activity and automatically notify relevant personnel. However, NALC HBP has not formally identified what constitutes an intrusion, and the system has not been configured to notify personnel.

NIST SP 800-53 Revision 4 requires an organization to develop, document and disseminate an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance as well as procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Recommendation 17

We recommend that NALC HBP develop and implement incident response policies and procedures in accordance with NIST SP 800-53 Revision 4.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-15 Incident Management Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has developed and implemented incident response policies and procedures in accordance with NIST guidance; no further action is required.

2. **Full Scope Vulnerability Scanning**

We conducted a review of NALC HBP's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate vulnerabilities.

NALC HBP has not implemented a thorough vulnerability scanning methodology to detect known weaknesses, and its server environment has only been subject to a single vulnerability scan. NIST SP 800-53 Revision 4 states that the organization should routinely scan "for vulnerabilities in the information system and hosted applications. . . ."

Failure to perform full scope vulnerability scanning increases the risk that NALC HBP's systems contain security vulnerabilities that could lead to sensitive data being stolen or destroyed.

Recommendation 18

We recommend that NALC HBP implement a methodology to routinely conduct vulnerability scans on its entire network environment, and to remediate vulnerabilities detected during scans in a timely manner.

NALC HBP Response:

"The NALC HBP has deployed a vulnerability scanning product from [redacted]

The product proactively scans our environment for misconfigurations, vulnerabilities and malware and provides guidance for mitigating risk.

An automated vulnerability scan is performed on all [redacted] ***on*** [redacted] ***A manual scan of*** [redacted] ***and other sensitive servers is performed on a*** [redacted] ***. Due to the sensitive nature of the*** [redacted] ***Systems, appropriate staff will be on site during the scan in the event of an issue. . . .***

Vulnerabilities are remediated in a timely manner according to their level of criticality.

A vulnerability trend report showing progress of the remediation process is emailed to appropriate staff on a monthly basis.

The NALC HBP policy is now formally documented in IS-10 Malicious Software Management Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process to routinely conduct vulnerability scans on the entire network environment. However, as part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence of the [redacted] scan reports, vulnerability tracking system, and evidence of remediation.

3. Vulnerabilities Identified by OIG Scans

System Patching

NALC HBP has not documented its patch management policies and procedures. The results of our vulnerability scans indicate that critical patches, service packs, and hot fixes are not implemented in a timely manner.

FISCAM states that "software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 4 requires that "The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously."

Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be compromised.

Recommendation 19

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

NALC HBP Response:

"The Plan deployed [redacted] in order to address this finding."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented procedures and software to ensure that its servers are updated with the appropriate patches, service packs, and hotfixes on a timely basis; no further action is required.

Configuration Weaknesses

The results of our vulnerability scans indicated that several servers were configured insecurely. The configurations contained known weaknesses that could be exploited maliciously.

FISCAM states that "software should be scanned and updated frequently to guard against known vulnerabilities."

Failure to securely configure servers to industry standards increases the risk of a successful malicious attack on the information system.

Recommendation 20 (from Flash Audit Alert issued July 29, 2013)

We recommend that NALC HBP make the appropriate changes to its computer servers in order to address the critical weaknesses identified in the vulnerability scans performed during this audit.

NALC HBP Response:

"All critical weaknesses discovered during the audit were addressed and remedied except for [redacted]. The [redacted] will be addressed as part of a larger [redacted] system upgrade which is being investigated at this time. Additionally the NALC HBP found that our [redacted] needs to be replaced for the reasons cited above. It is expected that the [redacted] will be replace by the end of 1st quarter 2014."

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence that all of the critical weaknesses identified in the vulnerability scans performed during the audit have been remediated or that the servers containing weaknesses have been replaced.

Noncurrent software

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

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

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

Recommendation 21

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

NALC HBP Response:

"Production servers will only have software installed that is deemed necessary for the role and management of the server. Application software is kept current by updating to the latest version as we are notified by the manufacturer. Unnecessary software installed on servers is removed when discovered in the [redacted], or upon being noticed in [redacted] reports. Patch Management [redacted] software will automatically update operating system and related necessary software ([redacted]

A [redacted] of the servers will be performed by the Information Systems Department to check for outdated and unnecessary software.

The NALC HBP policy is now formally documented in IS-11 Network Security Management Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a process to ensure that only current and supported versions of system software are installed on the production servers; no further action is required.

4. Unauthorized Devices

NALC HBP has not implemented controls to detect and prevent unauthorized devices from connecting to its internal network. The Plan's current process is to retroactively review the list of devices connected to the network and search for anomalies.

NIST SP 800-53 Revision 4 states that an organization should protect information on networks from unauthorized access.

Recommendation 22

We recommend that NALC HBP implement a control to prevent unauthorized devices from connecting to its internal network environment.

NALC HBP Response:

"A new firewall was deployed at the NALC HBP on January 24, 2014. The technician that installed the device has indicated that our firewall is capable of performing this service. It is expected that this service will be implemented in February 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a new firewall with the functionality to prevent unauthorized devices from connecting to the internal network environment; no further action is required.

5. Firewall Management

NALC HBP has implemented and utilizes a firewall to protect its network environment. However, a firewall policy, a routine compliance review process, and a firewall change control process have not been formally documented.

NIST SP 800-41 Revision 1 states that a firewall policy should dictate how firewalls handle network traffic based on the organization's information security policies, and a risk analysis should be performed to determine types of traffic needed by the organization. The policy should also include specific guidance on how to address changes to the rule set.

Failure to develop a firewall configuration policy and manage the settings increases the organization's exposure to unsecure traffic and vulnerabilities.

Recommendation 23

We recommend that NALC HBP develop a formal firewall management policy.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-11 Network Security Management Policy and will be effective on February 1, 2014.

Baseline configurations are being established as part of the implementation and training process for the new firewall."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has documented a formal firewall management policy; no further action is required.

Recommendation 24

We recommend that NALC HBP implement a process to conduct routine configuration compliance reviews of its network firewalls.

NALC HBP Response:

"As part of the new firewall implementation process, the technician performing the installation will assist in establishing configuration compliance review methodology."

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence when a process to conduct routine configuration compliance reviews on the firewalls has been implemented.

D. Configuration Management

System Software

NALC HBP's claims processing application [redacted] is housed on an [redacted] and additional supporting applications are housed in a [redacted]. We evaluated NALC HBP's configuration management of its [redacted] servers.

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

1. Configuration Management Policies and Procedures

NALC HBP has not developed configuration policies and procedures related to ensuring its computer servers are configured in a secure manner. In addition, NALC HBP has not documented a formal baseline configuration for its computer servers. A baseline configuration is a formally approved standard outlining how to securely configure various operating platforms.

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, as well as procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

In addition, NIST SP 800-53 Revision 4 states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk the system may not be configured in a secure manner.

Recommendation 25

We recommend that NALC HBP develop corporate configuration management policies and procedures in accordance with NIST SP 800-53 Revision 4 guidelines.

NALC HBP Response:

"The NALC HBP is in the process of documenting our configuration management policies and procedures in accordance with the NIST guidelines. As this requires research across many platforms and operating systems, the process has required more research and planning than we had anticipated. We are soliciting outside resources and reviewing compliance and monitoring products for the [redacted] side of our environment and are researching United States Government Baseline Configuration –National Checklist Program for our [redacted] policies and procedures.

We are targeting the second quarter 2014 for having management policies fully formed."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence when the plan has developed and implemented corporate configuration management policies and procedures in accordance with NIST guidance.

2. Configuration Compliance Auditing

As noted above, NALC HBP does not maintain approved operating platform security configurations, and therefore cannot effectively audit its systems security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53 Revision 4 states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system.

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 26

We recommend that NALC HBP document approved baseline configurations for all operating platforms.

NALC HBP Response:

"The NALCHBP has completed a [redacted] Compliance Assessment through an [redacted] focused third party company known as [redacted] as a first step toward establishing baseline configurations on that platform. We will be establishing a test partition of our production environment to assess the business impact of implementing the baseline configurations. Our IT staff is in the process of creating a test network environment in order to create a baseline [redacted] environment based upon United States Government Baseline Configuration –National Checklist Program recommendations."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence when the plan has documented an approved baseline configuration for all operating platforms.

Recommendation 27

We recommend that NALC HBP implement a process to routinely audit network servers' security configuration settings to ensure they are in compliance with the approved configuration baselines.

NALC HBP Response:

"The NALC HBP has entered into a contract with a third party known as [redacted] acquire an application that will monitor for assurance that security configurations are maintained according to established baselines. The NALC HBP has recently reviewed an application from [redacted] that will provide similar capabilities for monitoring the [redacted] A determination will be made regarding acquiring this application after product quotes are received."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence when the Plan has implemented a process to routinely audit network servers' security configuration settings to ensure compliance with the approved configuration baselines.

3. System Software Change Control

NALC HBP maintains a running list of changes made to [redacted] However, NALC HBP has not established a formal systems development lifecycle (SDLC) methodology with corporate approved policies and procedures. Although a list of system changes is maintained, relevant documentation related to the change is not maintained for post-implementation review.

NIST SP 800-53 Revision 4 recommends that organizations determine the types of changes to the information system that should be controlled, approve configuration changes to the system with consideration for security impact analysis, document approved configuration changes, retain and review records of configuration changes, audit activities associated with configuration changes, and coordinate and provide oversight for configuration change control.

Although all changes made to the system are documented, a formal policy outlining the required documentation and the required approvals for all system changes has not been developed. This exposes the system to unwarranted and unapproved changes, potentially leading to system vulnerabilities.

Recommendation 28

We recommend that NALC implement formal system software change control policies and procedures in accordance with NIST SP 800-53 Revision 4 to ensure that changes are approved, documented, recorded, reviewed, audited, and given oversight.

NALC HBP Response:

"The NALC HBP has not the resources currently to institute this recommendation but will be creating a testing environment for the [redacted] and a test network toward building a compliance platform. Configuration change control procedures will follow after baselines are established. Change Management Policy will be adjusted accordingly as the project

unfolds. In the meantime, changes will be reviewed documented and approved according to current procedures."

OIG Reply:

As part of the audit resolution process, we recommend that NALC HBP provide OPM's HIO with evidence when the plan has implemented formal system software change control policies and procedures in accordance with NIST guidance.

4. Password Requirements

NALC HBP has documented corporate password standards. However, we discovered many instances where information systems did not follow the established guidelines.

NIST SP 800-53 Revision 4 requires an organization to enforce minimum password complexity based on organization defined requirements.

Failure to enforce strong password requirements on information systems increases the risk that the systems could be breached by brute force password attacks.

Recommendation 29

We recommend that NALC HBP make the appropriate system changes to ensure that all systems require complex passwords that comply with the corporate policy.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-05 Account Management Policy and will be effective on February 1, 2014."

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with screen shots of the password configurations from the information systems indicating compliance with the new corporate password policy.

E. Contingency Planning

We reviewed NALC HBP's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur. We determined that the Plan has identified critical applications and routinely rotates back-up data to an off-site location. However, we have serious concerns about NALC HBP's contingency planning program and do not have confidence that the plan could maintain business operations if its primary facility was disabled.

The sections below document opportunities for improvement related to NALC HBP's contingency planning program.

a) Business Impact Analysis

NALC HBP has not conducted an adequate business impact analysis (BIA). During the field work phase of the audit we were provided with a draft version of a BIA, but it has not been finalized and does not contain several of the requirements documented in NIST 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems.

NALC HBP also has not identified the critical resources (i.e., personnel) required to support critical operations and business functions in the event of a disaster, nor has it identified recovery priorities. NALC HBP has created a list of critical hardware, but all items were equally assigned the highest priority.

NIST 800-34 Revision 1 states that a BIA is a key step in implementing a contingency planning process. Three steps involved in completing a BIA include determining business processes and recovery criticality, identifying resource requirements, and identifying recovery priorities for system resources. Failure to conduct a BIA increases the risk that the Plan will not be able to recover critical business operations in a timely manner.

Recommendation 30

We recommend that NALC HBP conduct a business impact analysis in accordance with NIST 800-34 Revision 1.

NALC HBP Response:

"For Recommendations 30-36 (also see individual recommendations for specific responses): The NALC HBP agrees generally with the OIG's overall assessment of the Plan's contingency planning program. Prior to the commencement of the OIG's audit of general and application controls, the Plan sought its own independent assessment of its disaster recovery and business continuity capabilities, which included the aforementioned draft business impact analysis. Senior management, upon reviewing the unfinalized draft report, chose to move aggressively to mitigate what it saw as the most critical weaknesses including the back-up data capabilities. Management remains committed to an aggressive mitigation strategy and a complete redesign of its contingency planning program, which will address all of the weaknesses identified by the OIG, including most significantly, the Plan's data back-up and alternate work site capabilities. Plan documentation and testing will follow accordingly in compliance with NIST and/or other best practices. At this time, while management has sought proposals for on-site back-up power generation, we feel other elements of the overall contingency plan redesign may obviate the need for this recommendation.

With respect to OIG's comment that the NALC HBP does not routinely perform emergency response training, we wish to clarify that while it is our intent to revisit and improve all areas of our contingency planning including emergency response training, the Plan does in fact routinely arrange for the members of its volunteer AED staff to recertify their CPR training."

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence once a business impact analysis has been conducted in accordance with NIST guidance. With regards to NALC HBP's plan to redesign its contingency planning program, we will work with HIO's audit resolution team to make the appropriate adjustments to the contingency planning related recommendations as the Plan develops its new strategy.

b) Alternate Recovery Location

NALC HBP does not have an alternate location to recover its computing environment in the event of a disaster. We were told that NALC HBP has made arrangements to begin using hardware at the NALC union headquarters building in Washington, D.C. as a backup location, and production data will be mirrored between the two sites. However, NALC HBP has not identified an alternate location for employees to work and perform business operations.

NIST SP 800-53 Revision 4 states that an organization must establish "an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions. . . ." Failure to establish an alternate processing site prohibits NALC HBP from continuing business operations in the event of a disaster.

Recommendation 31

We recommend that NALC HBP fully implement the data backup capabilities at the NALC headquarters building.

NALC HBP Response:

"In August of 2013 the NALC HBP conducted a major infrastructural upgrade to our IT environment in order to facilitate off-site data replication. A similar environment was constructed in October 2013 at our data exchange partner location, the National Association of Letter Carriers (NALC) Headquarters in Washington DC.

The components of the exchange infrastructure are an [redacted] are server environment and a [redacted] with a [redacted]. All of these components are established and operational at each location.

However, both sites encountered a problem with the [redacted] during installation. The problem proved to be an obscure one that was just finally resolved on January 17, 2014. The project could not entirely move forward until the issue was settled. In the interim, the NALC HBP IT staff attended week–long training sessions for the [redacted] in November 2013 and for the [redacted] elements of the solution in December 2013.

Additionally in December 2013, an [redacted] technician completed a configuration evaluation, firmware updates to relevant devices, and established network storage areas at this facility

and at NALC HQ for purposes of replication. The technician will be returning in February 2014 to complete the training and begin implementation.

The [redacted] server farm was established in November 2013 but this portion of the project was also placed on hold until the [redacted] issue was resolved. [redacted] training will be hands-on as the project unfolds.

It is anticipated that replication will be functioning fully in the March 2014 timeframe."

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence once it has fully implemented the data backup capabilities at the NALC headquarters building.

Recommendation 32

We recommend that NALC HBP create a plan that establishes an alternate work site for its employees that allows for critical business operations to continue if the main facility is not accessible.

NALC HBP Response:

Included in the NALC HBP response to recommendation 30.

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence once a plan has been established for an alternate work site that allows for critical business operations to continue in the event the main facility is inaccessible.

c) Data Center Generator

The backup power generator at the NALC HBP facility does not have the capacity to sustain the data center in the event of a prolonged power outage. NALC HBP has an uninterruptable power supply that can sustain the data center for up to four hours. However, any power outage lasting longer than four hours would result in the complete shutdown of operations until power could be restored. This issue is compounded by the lack of an alternate recovery location.

HIPAA §164.308(a)(7)(ii)(C) requires covered entities to "Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode." NALC HBP could not process claims if its facility experiences an extended power outage.

Recommendation 33

We recommend that NALC HBP install a power generator that can maintain data center operations in the event of a power loss.

NALC HBP Response:

Included in the NALC HBP response to recommendation 30.

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence once the Plan has installed a power generator that can maintain data center operations in the event of a power loss, or implemented other controls that would address the weaknesses described in this section.

d) Contingency Plan

NALC HBP's contingency plan does not address many of the suggested elements of NIST SP 800-34 Revision 1. NALC HBP has created a Disaster Recovery Manual that outlines high level procedures to follow in the event of a disaster. However, the procedures instruct disaster recovery personnel to perform actions and analysis that typically should be performed before a disaster occurs, and already be documented in a contingency plan. Also, the fact that NALC HBP has not conducted a BIA, established alternate recovery and processing locations, or identified critical resources drastically reduces the effectiveness of the Disaster Recovery Manual.

NIST SP 800-34 Revision 1 identifies the five main components of a contingency plan, as follows: Supporting Information, Activation and Notification Phase, Recovery Phase, Reconstitution Phase, and Appendices. Failure to establish a thorough contingency plan increases the risk that NALC HBP will not be able to continue business operations in the event of a disaster.

Recommendation 34

We recommend that NALC HBP update its Disaster Recovery Manual in accordance with NIST SP 800-34 Revision 1.

NALC HBP Response:

Included in the NALC HBP response to recommendation 30.

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence once the Disaster Recovery manual has been updated in accordance with NIST guidance.

e) Contingency Plan Testing

NALC HBP does not perform contingency plan testing. We were told that the Plan has at one time restored data from back-up tapes. However, the restoration occurred several years ago and was performed on the production environment at the main facility. NALC HBP has never restored data at an alternate location.

NIST SP 800-34 Revision 1 states that contingency plan testing "is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan." NIST SP 800-53 Revision 4 states that the organization must review the contingency plan test results and initiate corrective action. Failure to test the contingency plan increases the risk that NALC HBP will not be able to recover business operations if unexpected events occur.

Recommendation 35

We recommend that NALC HBP routinely test its contingency plan and incorporate the results into the contingency plan.

NALC HBP Response:

Included in the NALC HBP response to recommendation 30.

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence that the contingency plan is routinely tested and the results incorporated into plan updates.

f) Emergency Response Training

NALC HBP does not routinely perform emergency response training. The Plan conducts periodic evacuation drills and has procedures for activating the fire suppression system in the data center. However, there is no periodic training for employees with emergency response responsibilities.

NIST SP 800-53 Revision 4 states that the Plan should train "personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training." Failure to conduct periodic emergency response training would increase the risk that human life, equipment, and sensitive data would be lost.

Recommendation 36

We recommend that NALC HBP provide periodic emergency response training to individuals with emergency response responsibilities.

NALC HBP Response:

Included in the NALC HBP response to recommendation 30.

OIG Reply:

As part of the audit resolution process, we recommend that the Plan provide OPM's HIO with evidence that employees with emergency response responsibilities are provided periodic training relevant to their roles in business continuity and disaster recovery.

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting NALC HBP's claims adjudication process.

1. Application Configuration Management

System Development Life Cycle Methodology

NALC HBP has not implemented a standard SDLC methodology for managing application development. NALC HBP owns a change management software product, but usage policies and procedures have not been formally defined.

According to FISCAM, "The entity should have a documented SDLC methodology that details the procedures that are to be followed when applications are being developed, as well as when they are subsequently modified."

Failure to implement a standard SDLC methodology increases the risk that unapproved and improperly tested changes are introduced into the production environment.

Recommendation 37

We recommend that NALC HBP implement a formal SDLC methodology that defines responsibilities for each employee within the change control process. This process should require standardized documentation for all steps of the change control process.

NALC HBP Response:

"The NALC HBP policy is now formally documented in IS-30 System Development Lifecycle Policy and will be effective on February 1, 2014."

OIG Reply:

The evidence provided by NALC HBP in response to the draft audit report indicates that the Plan has implemented a formal SDLC methodology that defines responsibilities for each employee within the change control process. The process also includes standardized documentation for all steps of the change control process; no further action is required.

2. Claims Processing System

We evaluated the input, processing, and output controls associated with NALC HBP's claims processing system. We determined that NALC HBP has implemented policies and procedures to help ensure that:

- paper claims that are received in the mail room are tracked to ensure timely processing;
- claims are monitored as they are processed through the system; and
- claims scheduled for payment are actually paid.

3. Enrollment

We evaluated NALC HBP's procedures for managing its database of member enrollment data. Changes to member enrollment information are primarily received via an encrypted electronic transmission. Enrollment changes are processed on a weekly basis. NALC HBP has an audit function for each step of the enrollment process. We do not have any concerns regarding NALC HBP's enrollment policies and procedures.

4. Debarment

NALC HBP has adequate procedures for updating its claims system with debarred provider information. NALC HBP downloads the OPM OIG debarment list every month and converts the file to a format that is loaded into the Plan's claims processing system. Any debarred providers that appear in NALC HBP's provider database are flagged to prevent claims submitted by that provider from being inappropriately paid during the claims adjudication process. Nothing came to our attention to indicate that NALC HBP has not implemented adequate controls over the debarment process.

5. Application Controls Testing

We conducted a test on NALC HBP's claims adjudication application to evaluate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which NALC HBP's systems adjudicated the claims. Our test results indicated that NALC HBP's system has controls and system edits in place to identify the following scenarios:

- timely filing;
- enrollment inconsistencies;
- invalid date of service;
- chiropractic benefit structure;
- duplicate claims; and
- coordination of workers compensation.

The sections below document opportunities for improvement related to NALC's claims application controls.

a. Medical Editing

Our claims testing exercise identified several scenarios where NALC HBP's claims system failed to detect medical inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- [redacted]
- [redacted]

- [redacted]
- [redacted]
- [redacted]
  and
- [redacted]

These system weaknesses increase the risk that benefits are being paid for procedures that were not actually performed.

Recommendation 38

We recommend that NALC HBP make the appropriate system modifications to prevent medically inconsistent claims from being processed.

NALC HBP Response:

"For Recommendations 38-41: The original application control testing that was conducted on the Plan's claim system did not include all the processes that the Plan employs to adjudicate a claim, i.e., it was not conducted as an end-to-end test, but focused exclusively on the claim system. The attached spreadsheet (OIG Test Claims) lists the claims scenarios and includes comments from the Plan and Cigna which take into account our end-to-end claims process.

In addition, the Plan performs post-payment audits daily to ensure that claims are being adjudicated correctly. The audits performed by our internal Audit Department are described below. . . .

We believe that the process as a whole provides sufficient protections against the inappropriate payment of claims. In addition, the Plan is actively investigating the purchase of a clinically based claims audit program that applies edits to claims during the adjudication process as a further level of protection."

OIG Reply:

NALC HBP's response indicates that the application control testing performed during this audit did not properly reflect all the controls that the Plan employs to adjudicate a claim in the production environment. However, to date no evidence has been provided to support this position. If and when the Plan is able to provide evidence of the controls present in the end-to-end adjudication process, we will perform additional testing as part of a supplemental or follow-up audit. The recommendations in this section of the report should remain open until NALC HBP has successfully demonstrated that the weaknesses described do not exist in its claims processing system.

b. [redacted]

Test claims were processed that violate [redacted].

[redacted]

This system weakness increases the risk that benefits are being paid for procedures that were not actually performed.

Recommendation 39

We recommend that NALC HBP make the appropriate system modifications to enforce proper procedure code billing guidelines.

NALC HBP Response:

Included in the NALC HBP response to Recommendation 38.

OIG Reply:

As mentioned in the OIG Reply to Recommendation 38, if and when the Plan is able to provide evidence of the end-to-end system of controls, we will perform additional testing as part of a supplemental or follow-up audit.

c. [redacted]

NALC HBP's claims processing system paid [redacted] claims for a member with [redacted].

The system does not have edits in place to prevent duplicate [redacted] charges for [redacted]. We submitted two claims for [redacted] for one member at the same [redacted]. We also submitted claims for a member for [redacted] at [redacted] on [redacted] NALC HBP inappropriately processed and paid the duplicate services for both sets of claims.

This system weakness increases the risk that [redacted] are being paid for duplicate [redacted] expenses.

Recommendation 40

We recommend that NALC HBP make the appropriate system modifications to ensure that claims are not paid for duplicate [redacted] charges.

NALC HBP Response:

Included in the NALC HBP response to Recommendation 38.

OIG Reply:

As mentioned in the OIG Reply to Recommendation 38, if and when the Plan is able to provide evidence of the end-to-end system of controls, we will perform additional testing as part of a supplemental or follow-up audit.

d. [redacted]

Duplicate test claims were processed for a procedure that typically [redacted].

We submitted two test claims with a patient receiving a [redacted] on separate dates. These claims were processed and paid without encountering any edits. Due to the similarity of these claims, we expected the second claim to be deferred by a suspected duplicate edit, so that a claims processor could determine if the claim was submitted correctly.

Recommendation 41

We recommend that NALC HBP make the appropriate system modification to prevent near duplicate claims from processing.

NALC HBP Response:

Included in the NALC HBP response to Recommendation 38.

OIG Reply:

As mentioned in the OIG Reply to Recommendation 38, if and when the Plan is able to provide evidence of the end-to-end system of controls, we will perform additional testing as part of a supplemental or follow-up audit.

G. Health Insurance Portability and Accountability Act

We reviewed NALC HBP's efforts to maintain compliance with the security and privacy standards of HIPAA.

NALC HBP's HIPAA security and privacy organization consists of a security officer and privacy officer. The Plan developed a series of privacy policies and procedures that address requirements of the HIPAA privacy rule. NALC HBP reviews its HIPAA privacy and security policies annually and updates when necessary. However, all of the elements of the HIPAA security rule have not been implemented. The areas within the security rule that need to be improved have been discussed in the sections above. By implementing those recommendations, NALC HBP will be in compliance with the HIPAA security rule.

III. Major Contributors to This Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Chief
- [redacted], Auditor-In-Charge
- [redacted], Lead IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

Appendix I

July 29, 2013

MEMORANDUM FOR ELAINE KAPLAN
Acting Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Flash Audit Alert – Information Security at the National Association of Letter Carriers Health Benefit Plan (NALC HBP)

The U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) is issuing this flash audit alert to bring to your immediate attention serious concerns we have regarding the National Association of Letter Carriers Health Benefit Plan's (NALC HBP) ability to adequately secure sensitive Federal data.

NALC HBP is a participating carrier in the Federal Employees Health Benefits Program (FEHBP) and processes health insurance claims for FEHBP members and their dependents. This company therefore manages highly sensitive data such as personally identifiable information and personal health information.

We are currently in the fieldwork phase of an information technology (IT) audit at NALC HBP, and have determined that this organization has a very limited information security program. One primary concern is the fact that NALC HBP has not developed comprehensive IT security policies and procedures. IT policies and procedures are the critical foundation of a strong information security program, as these documents provide guidance on how IT security should be managed at a specific organization.

We also conducted vulnerability scans of NALC HBP's network server environment, and discovered critical vulnerabilities that could be easily exploited by a malicious attacker. These weaknesses include, but are not limited to: insecure server configurations, outdated and unnecessary software installations, and missing vendor security patches and hot fixes.

In addition to these two primary concerns, we detected the following serious or critical weaknesses in NALC HBP's information security program:

- A lack of IT security training for employees;
- Weak physical access controls to facilities and sensitive computing resources;
- No formal system development life cycle methodology;
- Weak system authentication requirements;

- Under-developed business continuity and disaster recovery strategies; and,
- Inadequate management of system software configuration.

Most, if not all, of these findings are a direct violation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

We plan to issue a full IT audit report (*Audit of Information System General & Application Controls at NALC HBP*, Report No. 1B-32-00-13-037) that will contain many specific audit recommendations to improve IT security at NALC HBP. However, this report will not be issued until fiscal year 2014, and we are therefore immediately issuing the following recommendations so that NALC can begin taking steps to address the most serious weaknesses.

Recommendation 1

We recommend that NALC HBP develop comprehensive IT security policies and procedures. At a minimum, NALC HBP should implement policies and procedures related to the following topics:

- Risk Assessments
- Contingency Planning and Testing
- Security Awareness Training
- Employee Termination
- Physical Access Controls
- Auditing/Monitoring User and Administrator Activity
- Appropriate Use of Software
- Segregation of Duties
- Security Incident Response
- Password Requirements
- Vulnerability Scanning
- Server Configuration Management, Baseline Configurations, and Auditing Server Configuration
- System Development Lifecycle
- Firewall Management
- Web and E-mail Filtering
- Wireless Network Access
- Control of Removable Media

Recommendation 2

We recommend that NALC HBP make the appropriate changes to its computer servers in order to address the critical weaknesses identified in the vulnerability scans.

If you have any questions about this flash audit alert you can contact me at 606-1200, or your staff may wish to contact Michael R. Esser, Assistant Inspector General for Audits, at 606-2143.

cc: Elizabeth A. Montoya
Chief of Staff

John O'Brien
Director, Healthcare and Insurance

Shirley R. Patterson
Assistant Director for Federal Employee Insurance Operations

[redacted]
Associate Director, Merit System Audit and Compliance

[redacted]
Director, Internal Oversight & Compliance

Appendix II

NATIONAL ASSOCIATION OF LETTERS CARRIERS

HEALTH BENEFIT PLAN

20547 Waverly Court, Ashburn, Virginia 20149 • (703)729-4677 or 1-888-636-NALC (6252)
Fredric V. Rolando, President • **Brian E. Hellman,** Director

January 31, 2014

[redacted]
Auditor-In-Charge
Information Systems Audits Group
United States Office of Personnel Management
Office of the Inspector General

Dear [redacted]:

Enclosed please find the NALC Health Benefit Plan's comments and responses to the draft report detailing the results of the audit of general and application controls over the information systems, conducted at our offices by the Office of the Inspector General at the U.S. Office of Personnel Management (OPM).

In general, our comments and responses align to specific recommendations made in the draft report. However, with respect to the sections addressing Contingency Planning and Claims Adjudication, our comments respond to the general findings and are organized under a single heading. Where references are made to supporting documentation, we have included those as separate attachments in either MS Word or Excel format.

If you should have any questions, please feel free to contact me at [redacted] or [redacted].

[redacted]
Administrator
NALC Health Benefit Plan

cc: [redacted]

Recommendation 1 (from Flash Audit Alert issued July 29, 2013)

We recommend that NALC HBP develop comprehensive IT security policies and procedures. At a minimum, NALC HBP should implement policies and procedures related to the following topics:

- Risk Assessments
- Contingency Planning and Testing
- Security Awareness Training
- Employee Termination
- Physical Access Controls
- Auditing/Monitoring User and Administrator Activity
- Appropriate Use of Software
- Segregation of Duties
- Security Incident Response
- Password Requirements
- Vulnerability Scanning
- Server Configuration Management, Baseline Configurations, and Auditing Server Configuration
- System Development Lifecycle
- Firewall Management
- Web and E-mail Filtering
- Wireless Network Access
- Control of Removable Media

NALC HBP Response:

The NALC HBP has developed and adopted the attached Information Security Policies and Procedures.

Recommendation 2

We recommend that NALC HBP implement a process to routinely review and update its IT security policies.

NALC HBP Response:

The NALC HBP has established an Information Security Management Committee.

The committee members are: NALC HBP Director, the NALC HBP Administrator, the Human Resources Manager, the Facilities Manager, the Information Systems Manager, the Claims Superintendent, the HIPAA Security Officer and the HIPAA Privacy Official.

The committee, in conjunction with members of the Information Systems Department staff and representatives from the Administrative and Claims departments, have been integral in formulating the newly established policies. The committee will meet annually prior to the scheduled risk assessment to review and update IT security policies.

Policies will be addressed accordingly if circumstances dictate a review and update prior to the scheduled event.

The NALC HBP policy is now formally documented in IS-01 Information Security Program Policy on Policies and will be effective on February 1, 2014.

Recommendation 3

We recommend that as part of its efforts to obtain compliance with the HIPAA security rule, NALC HBP implement a security awareness training program for its employees. For

guidance in creating a security awareness program see NIST SP 800-50. The program should be managed by the security management structure.

NALC HBP Response:
The NALC HBP is in the process of creating a security awareness program based upon our own policies in conjunction with outside resources. Specifically we have contacted [redacted] regarding their – [redacted] educational suite and [redacted] regarding their [redacted]. Upon selection of the appropriate product, we will incorporate pertinent materials into our security program.

We are anticipating an April 2014 launch for our security awareness training program for all employees and will update our new employee educational material to address the security requirements.

Recommendation 4

We recommend that NALC HBP develop and implement a training program for employees with IT security responsibilities. The program should include:

- A process to identify and categorize positions with security responsibilities;
- Development of specialized security training requirements within job descriptions,
- Opportunities to seek and maintain technical certifications;
- Documentation of training completed by each employee; and
- A periodic review of employee records to ensure that specialized security training is completed in accordance with standards.

NALC HBP Response:
The NALC HBP is reviewing outside sources for purposes of establishing specialized training for employees with IT security responsibilities, which will include the bulleted items above. The sources contacted to date are [redacted].

The NALC HBP has always encouraged and has a documented history of allowing our employees opportunities to seek and maintain technical certifications.

Recommendation 5

We recommend that NALC HBP develop and implement a risk management policy and a risk assessment methodology. NIST SP 800-30 serves as an excellent reference to assist NALC HBP with the development of its risk management program. Implementation of the suggested framework would also help NALC HBP obtain compliance with the HIPAA Security Rule.

NALC HBP Response:
The NALC HBP policy is now formally documented in IS-19 IT Risk Management Policy and will be effective on February 1, 2014.

Recommendation 6

We recommend that NALC HBP implement a password policy that closely reflects industry standards.

NALC HBP Response:
The NALC HBP policy is now formally documented in IS-05 Account Management Policy and will be effective on February 1, 2014. We believe the policy provides appropriate safeguards in light of NALC HBP's business needs.

Recommendation 7

We recommend that NALC HBP address its [redacted] and [redacted] password setting weaknesses once a standard password policy has been implemented for the organization.

NALC HBP Response:
The NALC HBP policy is now formally documented in IS-05 Account Management Policy and will be effective on February 1, 2014.

Recommendation 8

We recommend that NALC HBP establish unique user accounts for each privileged user.

NALC HBP Response:
The NALC HBP has created unique user accounts for privileged users. At present, three Information Systems staff senior managers have unique privileged accounts on the network and on the [redacted] The Network Administrator has a unique privileged account on the network but not on the [redacted] The Programming Staff members have a lesser set of privileges on the [redacted] than the senior managers but no special network privileges. The Operations staff has a unique set of privileges on the [redacted] that are different than the programming staff and lesser than the senior managers and have a unique set of privileges on the network that are lesser than the senior managers.

The NALC HBP policy is now formally documented in IS-04 Access Control Policy and will be effective on February 1, 2014.

Recommendation 9

We recommend that NALC HBP implement a process to routinely review privileged user activities.

NALC HBP Response:
We have contracted with a third-party to provide an appliance and application that will allow them to monitor account activity on our behalf. This will provide real-time alerts based upon the sensitivity settings and will allow immediate review as required. A full review will be conducted weekly by internal and/or the third party sources.

The NALC HBP policy is now formally documented in IS-18 Monitoring and Log Management Policy.

It is expected that this process will be in place by February or March 2014.

Recommendation 10

We recommend that NALC HBP implement a process to review logical access to all of its systems and supporting applications to ensure that no terminated individuals retain access.

NALC HBP Response:

A list of all active employees will be forwarded to the Information Systems Department by the Human Resources department on a [redacted] basis. The Information Systems Department will compare the list against active network accounts and active [redacted] accounts for accuracy. Accounts will be adjusted accordingly.

Documentation of the review will be retained in the Human Resources Department.

The NALC HBP policy is now formally documented in IS-04 Access Control Policy and will be effective on February 1, 2014.

Recommendation 11

We recommend that NALC HBP implement a process to review appropriate level of access for active user accounts for all applications used to gain access to sensitive data.

NALC HBP Response:

The Information Systems Department will conduct [redacted] review of all network accounts for appropriate levels of access. The NALC HBP is assessing a monitoring tool from [redacted] for [redacted] accounts to ensure appropriate levels of access. The Information Systems Department will compare the list against active network accounts and active [redacted] accounts for accuracy. Accounts will be adjusted accordingly.

The NALC HBP policy is now formally documented in IS-04 Access Control Policy and will be effective on February 1, 2014.

Recommendation 12

We recommend that NALC HBP improve the physical access controls at its data center. At a minimum the computer room entrance should require multi-factor authentication and piggybacking controls at both entrances.

NALC HBP Response:

The NALC HBP is in agreement and is soliciting proposals from qualified vendors to augment the current physical access controls at its data center to include multi-factor authentication and alarm-based anti-piggyback controls at both entrances.

Recommendation 13

We recommend that NALC HBP implement a process for routinely auditing all active access cards to ensure that they are not assigned to terminated employees.

NALC HBP Response:

A list of all active access cards will be forwarded by the facilities manager on [redacted] basis to Human Resources to ensure

- **Cards are issued to active employees only**
- **Access level is appropriate for duties**
- **Card number corresponds with ID number**

The review of active access cards will be conducted by the Human Resources Department staff and a log of the event review will be maintained in that department.

The NALC HBP policy is now formally documented in IS-12 Physical Access Security Policy and will be effective on February 1, 2014. These are also reflected in HR Policies and Procedures Manual.

Recommendation 14

We recommend that NALC HBP implement a process to routinely recertify that employees with specialized access still require specialized access. If no specialized access is required, then the access level should be adjusted accordingly.

NALC HBP Response:

A list of all specialized Access Cards will be forwarded on a [redacted] basis to the Administrative Office for review or more frequently as changes become necessary. Upon review, specialized access will be adjusted accordingly.

Documentation of the review will be retained in the Human Resources Department.

The NALC HBP policy is now formally documented in IS-12 Physical Access Security Policy and will be effective on February 1, 2014. These are also reflected in HR Policies and Procedures Manual.

Recommendation 15

We recommend that NALC HBP implement a process to automatically disable temporary access badges.

NALC HBP Response:

Temporary cards are activated upon request from Human Resources when an employee forgets their permanent access badge. Our current system is unable to deactivate automatically. An RFI is being solicited for upgrade/replacement of Access System.

In the interim, temporary cards are deactivated [redacted].

The NALC HBP policy is now formally documented in IS-12 Physical Access Security Policy and will be effective on February 1, 2014. These are also reflected in HR Policies and Procedures Manual.

Recommendation 16

We recommend that NALC HBP reassess the physical access controls at its facility and implement controls that will ensure proper physical security. At a minimum, NALC HBP should implement a piggybacking control at the two main entrances to the facility.

NALC HBP Response:

The NALC HBP acknowledges the concern and has been actively investigating potential solutions to address the piggybacking issue highlighted by the OIG. While similar in nature to the concern raised with respect to the data center controls, we have determined the approach must be different due to the higher volume of employees passing through these entrances, and may involve the use of a turnstile or similar system. Any modification of the two main entrances of this nature must also be fully ADA compliant, will require building owner authorization and the appropriate building code permits.

Recommendation 17

We recommend that NALC HBP develop and implement incident response policies and procedures in accordance with NIST SP 800-53 Revision 4, IR-1, Incident Response Policy and Procedures.

NALC HBP Response:

The NALC HBP policy is now formally documented in IS-15 Incident Management Policy and will be effective on February 1, 2014.

Recommendation 18

We recommend that NALC HBP implement a process to routinely conduct vulnerability scan ing on the entire network environment and remediate vulnerabilities detected during scans in a timely manner.

NALC HBP Response:

The NALC HBP has deployed a vulnerability scanning product from [redacted] known as [redacted]

The product proactively scans our environment for misconfigurations, vulnerabilities and malware and provides guidance for mitigating risk.

An automated vulnerability scan is performed on [redacted]. A manual scan of [redacted] is performed on a [redacted]. Due to the sensitive nature of the [redacted], appropriate staff will be on site during the scan in the event of an issue.

Discovered vulnerabilities are reviewed a d placed into the following 5 categories:

Vulnerabilities are remediated in a timely manner according to their level of criticality.

A vulnerability trend report showing progress of the remediation process is emailed to appropriate staff on a monthly basis.

The NALC HBP policy is now formally documented in IS-10 Malicious Software Management Policy and will be effective on February 1, 2014.

Recommendation 19

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

NALC HBP Response:
The Plan deployed [redacted] in order to address this finding.

Service packs, security patches, and hotfixes [redacted] and routinely used 3rd party software such as [redacted], etc. are installed on the following schedule:

[redacted]

Recommendation 20 (from Flash Audit Alert issued July 29, 2013)

We recommend that NALC HBP make the appropriate changes to its computer servers in order to address the critical weaknesses identified in the vulnerability scans performed during this audit.

Noncurrent software

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

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

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

NALC HBP Response:
All critical weaknesses discovered during the audit were addressed and remedied except for the [redacted] will be addressed as part of a larger [redacted] which is being investigated at this time. Additionally the NALC HBP found that our [redacted] needs to be replaced for the reasons cited above. It is expected that the [redacted] will be replaced by the end of 1st quarter 2014.

Recommendation 21

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

NALC HBP Response:

Production servers will only have software installed that is deemed necessary for the role and management of the server. Application software is kept current by updating to the latest version as we are notified by the manufacturer. Unnecessary software installed on servers is removed when discovered in the [redacted] or upon being noticed in [redacted] or [redacted] reports. [redacted] software will automatically update operating system and related necessary software [redacted]

A [redacted] audit of the servers will be performed by the Information Systems Department to check for outdated and unnecessary software.

The NALC HBP policy is now formally documented in IS-11 Network Security Management Policy and will be effective on February 1, 2014.

Recommendation 22

We recommend that NALC HBP implement a control to prevent unauthorized devices from connecting to the internal network environment.

NALC HBP Response:

A new firewall was deployed at the NALC HBP on January 24, 2014. The technician that installed the device has indicated that our firewall is capable of performing this service. It is expected that this service will be implemented in February 2014.

Recommendation 23

We recommend that NALC HBP document formal firewall management policies.

NALC HBP Response:

The NALC HBP policy is now formally documented in IS-11 Network Security Management Policy and will be effective on February 1, 2014.

Baseline configurations are being established as part of the implementation and training process for the new firewall.

Recommendation 24

We recommend that NALC HBP implement a process to conduct routine configuration compliance reviews on its network firewalls.

NALC HBP Response:

As part of the new firewall implementation process, the technician performing the installation will assist in establishing configuration compliance review methodology.

Recommendation 25

We recommend that NALC HBP develop corporate configuration management policies and procedures in accordance with NIST SP 800-53 Revision 4 guidelines.

NALC HBP Response:

The NALC HBP is in the process of documenting our configuration management policies and procedures in accordance with the NIST guidelines. As this requires research across many platforms and operating systems, the process has required more research and planning than we had anticipated. We are soliciting outside resources and reviewing compliance and monitoring products for the [redacted] side of our environment and are researching United States Government Baseline Configuration –National Checklist Program for our [redacted] policies and procedures.

We are targeting the second quarter 2014 for having management policies fully formed.

Recommendation 26

We recommend that NALC HBP document approved baseline configurations for all operating platforms.

NALC HBP Response:

The NALCHBP has completed a [redacted] Assessment through an [redacted] focused third party company known as [redacted] as a first step toward establishing baseline configurations on that platform. We will be establishing a test partition of our production environment to assess the business impact of implementing the baseline configurations. Our IT staff is in the process of creating a test network environment in order to create a baseline [redacted] environment based upon United States Government Baseline Configuration – National Checklist Program recommendations.

Recommendation 27

We recommend that NALC HBP implement a process to routinely audit network servers' security configurations settings to ensure they are in compliance with the approved configuration baselines.

NALC HBP Response:

The NALC HBP has entered into a contract with a third party known as [redacted] to acquire an application that will monitor for assurance that security configurations are maintained according to established baselines.

The NALC HBP has recently reviewed an application from [redacted] will provide similar capabilities for monitoring the [redacted] A determination will be made regarding acquiring this application after product quotes are received.

Recommendation 28

We recommend that NALC implement formal system software change control policies and procedures in accordance with NIST SP 800-53, CM-3 Configuration Change Control, to ensure that changes are approved, documented, recorded, reviewed, audited, and given oversight.

NALC HBP Response:

The NALC HBP has not the resources currently to institute this recommendation but will be creating a testing environment for the [redacted] and a test network toward building a compliance platform. Configuration change control procedures will follow after baselines are established. Change Management Policy will be adjusted accordingly as the project unfolds. In the meantime, changes will be reviewed documented and approved according to current procedures.

Recommendation 29

We recommend that NALC HBP make the appropriate system changes to ensure that all systems require complex passwords that comply with the corporate policy.

NALC HBP Response:

The NALC HBP policy is now formally documented in IS-05 Account Management Policy and will be effective on February 1, 2014.

Recommendation 30

We recommend that NALC HBP conduct a business impact analysis in accordance with NIST 800-34 Revision 1.

NALC HBP Response for Recommendations 30-36 (also see individual recommendations for specific responses):

The NALC HBP agrees generally with the OIG's overall assessment of the Plan's contingency planning program. Prior to the commencement of the OIG's audit of general and application controls, the Plan sought its own independent assessment of its disaster recovery and business continuity capabilities, which included the aforementioned draft business impact analysis. Senior management, upon reviewing the unfinalized draft report, chose to move aggressively to mitigate what it saw as the most critical weaknesses including the back-up data capabilities. Management remains committed to an aggressive mitigation strategy and a complete redesign of its contingency planning program, which will address all of the weaknesses identified by the OIG, including most significantly, the Plan's data back-up and alternate work site capabilities. Plan documentation and testing will follow accordingly in compliance with NIST and/or other best practices. At this time, while management has sought proposals for on-site back-up power generation, we feel other elements of the overall contingency plan redesign may obviate the need for this recommendation.

With respect to OIG's comment that the NALC HBP does not routinely perform emergency response training, we wish to clarify that while it is our intent to revisit and improve all areas of our contingency planning including emergency response training, the Plan does in fact routinely arrange for the members of its volunteer AED staff to recertify their CPR training.

Recommendation 31

We recommend that NALC HBP fully implement the data backup capabilities at the NALC headquarters building.

NALC HBP Response:
In August of 2013 the NALC HBP conducted a major infrastructural upgrade to our IT environment in order to facilitate off-site data replication. A similar environment was constructed in October 2013 at our data exchange partner location, the National Association of Letter Carriers (NALC) Headquarters in Washington DC.

The components of the exchange infrastructure are an [redacted] with a [redacted] All of these components are established and operational at each location.

However, both sites encountered a problem with the [redacted] during installation. The problem proved to be an obscure one that was just finally resolved on January 17, 2014. The project could not entirely move forward until the issue was settled. In the interim, the NALC HBP IT staff attended week–long training sessions for the [redacted] November 2013 and for the [redacted] elements of the solution in December 2013.

Additionally in December 2013, [redacted] completed a configuration evaluation, firmware updates to relevant devices, and established network storage areas at this facility and at NALC HQ for purposes of replication. The technician will be returning in February 2014 to complete the training and begin implementation.

The [redacted] server farm was established in November 2013 but this portion of the project was also placed on hold until the [redacted] issue was resolved. [redacted] training will be hands-on as the project unfolds.

It is anticipated that replication will be functioning fully in the March 2014 timeframe.

Recommendation 32

We recommend that NALC HBP create a plan that establishes an alternate work site and allows for critical business operations to continue if the main facility is not accessible.

NALC HBP Response:
Included in NALC HBP Response to Recommendation 30 and 31

Recommendation 33

We recommend that NALC HBP install a power generator that can maintain data center operations in the event of a power loss.

NALC HBP Response:
Included in NALC HBP Response to Recommendation 30 and 31

Recommendation 34

We recommend that NALC HBP update its Disaster Recovery Manual in accordance with NIST SP 800-34 Revision 1.

Included in NALC HBP Response to Recommendation 30 and 31

Recommendation 35

We recommend that NALC HBP routinely test its contingency plan and incorporate the results into the contingency plan.

NALC HBP Response:

Included in NALC HBP Response to Recommendation 30 and 31

Recommendation 36

We recommend that NALC HBP provide periodic emergency response training to individuals with emergency response responsibilities.

NALC HBP Response:

Included in NALC HBP Response to Recommendation 30 and 31

Recommendation 37

We recommend that NALC HBP implement a formal SDLC methodology, which defines responsibilities for each employee within the change control process. This process should require standardized documentation for all steps of the change control process.

NALC HBP Response:

The NALC HBP policy is now formally documented in IS-30 System Development Lifecycle Policy and will be effective on February 1, 2014.

Recommendation 38

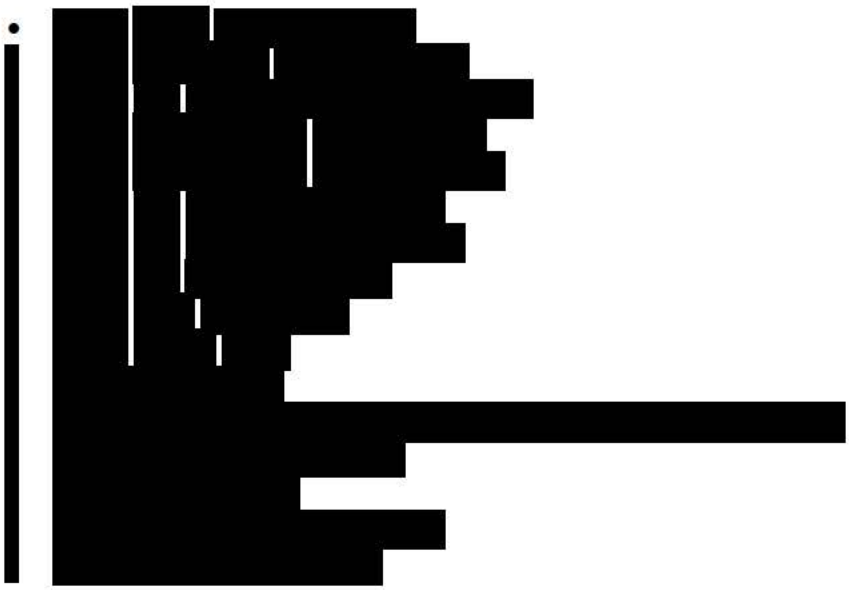
We recommend that NALC HBP make the appropriate system modifications to prevent medically inconsistent claims from being processed.

NALC HBP Response for Recommendations 38-41:

The original application control testing that was conducted on the Plan's claim system did not include all the processes that the Plan employs to adjudicate a claim, i.e., it was not conducted as an end-to-end test, but focused exclusively on the claim system. The attached spreadsheet (OIG Test Claims) lists the claims scenarios and includes comments from the Plan and Cigna which take into account our end-to-end claims process.

In addition, the Plan performs post-payment audits daily to ensure that claims are being adjudicated correctly. The audits performed by our internal Audit Department are described below.

The Audit department handles auditing of different types of claims that are processed by keyers, analysts, and the system. They detect errors in claims processed by any of these three sources. Each Audit analyst is assigned a unique identification number when auditing claims. The following are the types of audits that are performed on a daily basis:



On a rotating basis, the Audit department checks work done by employees in training and refresher classes. All analysts involved in the claims payment process have their work audited once every six months. Supervisors may request audits be done on their analysts if they feel they having trouble in a particular area.

While we believe that the process as a whole provides sufficient protections against the inappropriate payment of claims. In addition, the Plan is actively investigating the purchase of a clinically based claims audit program that applies edits to claims during the adjudication process as a further level of protection.

Recommendation 39

We recommend that NALC HBP make the appropriate system modifications to enforce proper procedure code billing guidelines.

NALC HBP Response:

Included in NALC HBP Response to Recommendation 38

Recommendation 40

We recommend that NALC HBP make the appropriate system modifications to ensure that claims are not paid for duplicate room and board charges.

NALC HBP Response:

Included in NALC HBP Response to Recommendation 38

Recommendation 41

We recommend that NALC HBP make the appropriate system modification to prevent near duplicate claims from processing.

NALC HBP Response:

Included in NALC HBP Response to Recommendation 38