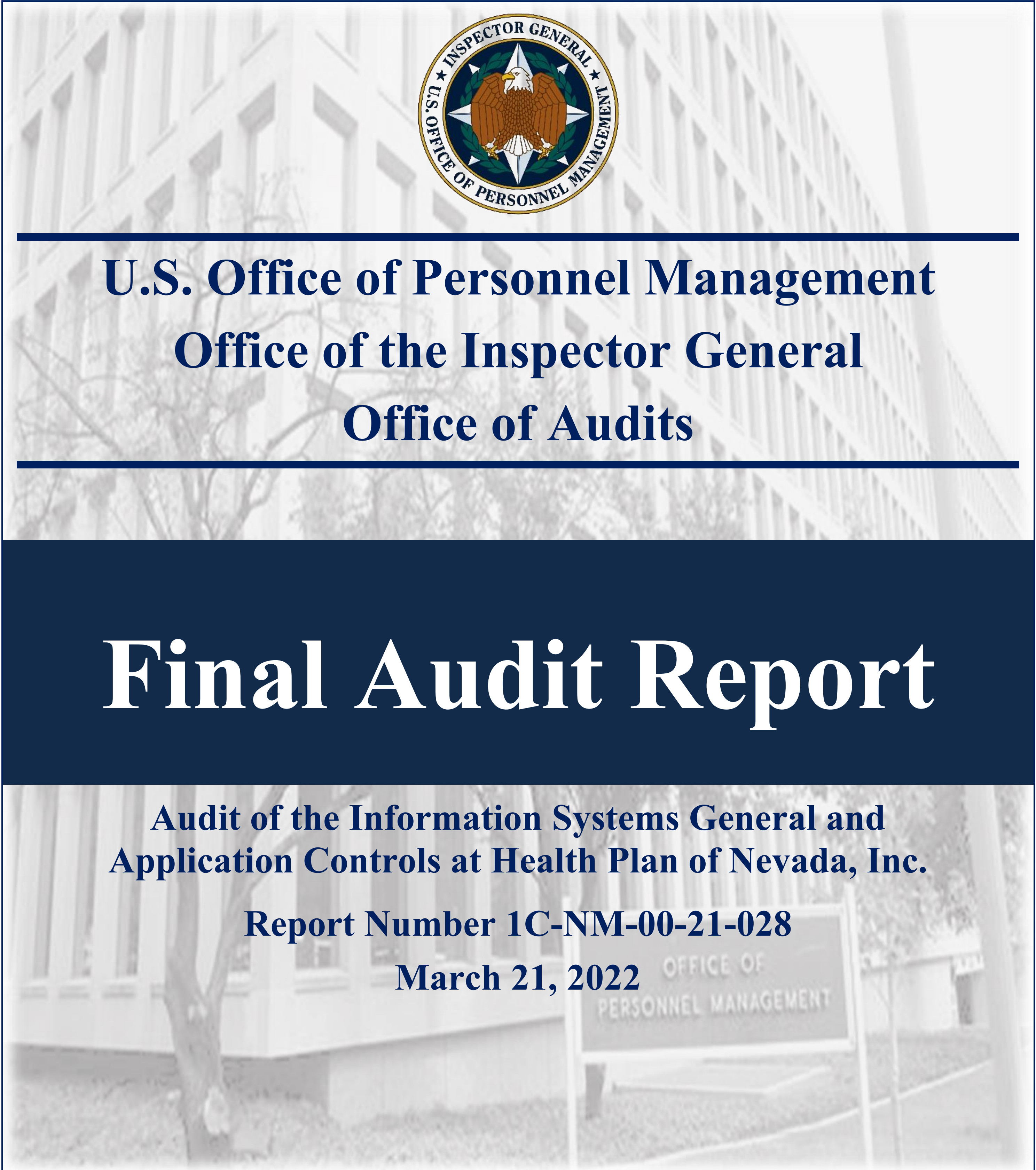

U.S. Office of Personnel Management
Office of the Inspector General
Office of Audits

Final Audit Report

Audit of the Information Systems General and Application Controls at Health Plan of Nevada, Inc.

Report Number 1C-NM-00-21-028
March 21, 2022

Executive Summary

Audit of the Information Systems General and Application Controls at Health Plan of Nevada, Inc.

Report No. 1C-NM-00-21-028 **March 21, 2022**

Why Did We Conduct the Audit?

Health Plan of Nevada, Inc. (HPN) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in HPN's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by HPN to process and store data related to medical encounters and insurance claims for FEHBP members**.**

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

Our audit of HPN's IT security controls determined that:

- HPN has an adequate security management program in place.
- Multi-factor authentication is not in place to access elevated IT passwords.
- HPN's primary data center does not have multi-factor authentication or anti-piggybacking controls in place.
- Some technical weaknesses exist in HPN's network environment.
- The enterprise security event monitoring and incident response programs are adequate.
- Compliance testing revealed that some systems are out of compliance with HPN's security configuration standards.
- The contingency planning program is adequate.
- HPN has adequate application change control policies and procedures.

Abbreviations

CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
HPN	**Health Plan of Nevada, Inc.**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology Special Publication**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**

Table of Contents

I. Background

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Health Plan of Nevada, Inc. (HPN).

The audit was conducted pursuant to FEHBP contract CS 1942; 5 U.S.C. Chapter 89, and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

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

HPN is a subsidiary of the UnitedHealth Group, which offers a wide range of health care products and services in addition to its FEHBP line of business. This was our initial audit of the information technology (IT) general security and application controls at HPN. All HPN personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit were greatly appreciated.

II. Objectives, Scope, and Methodology

Objectives

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

- Security management;
- Access controls;
- Network security;
- Security event monitoring and incident response;
- Configuration management;
- Contingency planning; and
- Application controls specific to HPN's claims processing system.

Scope and Methodology

This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of HPN'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 HPN'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 HPN to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Las Vegas, Nevada.

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

In conducting our audit, we relied to varying degrees on computer-generated data provided by HPN. 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.

We used judgmental, random selection, or statistical sampling methods as appropriate throughout the audit. Results of judgmentally or randomly selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

In conducting this audit, we:

- Performed a risk assessment of HPN's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM);
- Gathered documentation and conducted interviews;
- Reviewed HPN's business structure and environment; and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended.

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

- GAO's FISCAM, and
- National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

Compliance with Laws and Regulations

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

III. Audit Findings and Recommendations

A. Security Management

The security management component of this audit involved an examination of the policies and procedures that serve as the foundation of HPN's overall IT security program. We evaluated HPN's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

HPN has developed adequate IT security policies and procedures. HPN has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.

Nothing came to our attention to indicate that HPN has not implemented adequate security management controls.

B. Access Controls

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

We examined the physical access controls at HPN's facilities and data centers. We also examined the logical access controls protecting sensitive data on HPN's network environment and applications.

We observed the following controls in place:

- Routine access audits for secure areas;
- Procedures for appropriately granting and removing physical access to facilities and data centers; and
- Procedures for appropriately granting and adjusting logical access to applications and software resources.

The following sections document opportunities for improvement related to HPN's access management controls.

1. Identification and Authentication

HPN stores elevated passwords in a password vaulting tool. To retrieve the elevated passwords, personnel with IT administrative duties must authenticate to the vaulting tool with a username and password. The password vaulting tool is not configured for multi-factor authentication. HPN is aware of the gap and has a project in place to upgrade its tool to require multi-factor authentication in the near future.

HPN's password vaulting tool is not configured for multi-factor authentication.

NIST SP 800-53, Revision 5, states that organizations should "Implement multi-factor authentication for access to privileged accounts."

Failure to require multi-factor authentication to access privileged accounts increases the risk that threat actors may access privileged credentials.

Recommendation 1:

We recommend that HPN complete its project to require multi-factor authentication in order to access privileged credentials.

HPN's Response:

"The Plan completed multi-factor authentication on October 26, 2021. Proof of the implementation has been provided as Attachment 1 to this response."

OIG Comments:

In response to the draft audit report, HPN provided evidence that its vaulting tool is configured to require multi-factor authentication. The intent of this recommendation has been addressed. No further action is required.

2. Data Center Physical Access Controls

The primary data center is located in HPN's main office building. Access to the entrance of the office building requires a valid access card and is monitored by a security guard. However, the entrance to the data center is only controlled by an electronic badge reader and video surveillance. While this facility houses only HPN employees, not all of the employees who work in the building are authorized to access the data center where sensitive information systems reside. Therefore, we have identified the following improvements to the data center physical access controls that are considered industry best practices and that we have observed at the majority of FEHBP carriers that we audit:

- A technical or physical control to detect or prevent piggybacking (e.g., turnstiles, piggybacking alarms, two-door “man traps,” etc.); and

- Multi-factor authentication (e.g., electronic badge reader and pin number, biometric identification and pin number, etc.).

NIST SP 800-53, Revision 5, provides guidance for adequately controlling physical access to information systems containing sensitive data.

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

Recommendation 2:

We recommend that HPN implement piggybacking prevention controls at the entrance to its primary data center.

HPN’s Response:

“The plan updated its Policy to include the process by which employees gain access to the data center and specifically prohibits piggybacking by requiring each person to swipe their badge to gain access to the data center. Proof of the new policy has been provided as Attachment 2 to this response.”

OIG Comments:

HPN provided evidence that an administrative control is now in place to prohibit piggybacking. While HPN’s policy has been updated, the intent of the recommendation is to implement a technical or physical control to prevent or detect piggybacking. As described in the body of the report, the examples of technical and physical controls would provide increased security over an administrative policy update.

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

Recommendation 3:

We recommend that HPN implement multifactor authentication at the entrance to its primary data center.

HPN's Response:

"The Plan has evaluated the best method of multi-factor authentication at the entrance to its primary data center and determined that most effective method is the installation of cypher locks on both external doors to the data center. Additionally, the Plan is updating the security policy to definitively require guest logging with violations of the policy resulting in corrective actions up to an[d] including termination. The target for completion of the installation of the cypher locks is by January 31, 2022."

C. Network Security

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. We evaluated HPN's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during the audit.

We observed the following controls in place:

- Network access controls to prevent non-company devices from connecting to the network;
- A deny all, permit by exception firewall policy is in place; and
- Routine firewall reviews to ensure all rules are necessary.

The following section documents an opportunity for improvement related to HPN's network security controls.

1. Vulnerability Management

HPN conducted credentialed vulnerability and configuration compliance scans on a sample of servers in its network environment on our behalf. We chose a sample of [redacted] servers [redacted]. The sample included a variety of system functionality and operating systems across production, test, and development environments. The judgmental sample was drawn from systems that store and/or process Federal Member Data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population. The specific vulnerabilities that we identified were provided to HPN in the form of an audit inquiry but will not be detailed in this report. HPN was already aware of most of the identified technical weaknesses and had ongoing projects to

HPN has some technical weaknesses in its network environment.

remediate the vulnerabilities. HPN should continue working to complete its mitigation plans for the vulnerabilities we identified.

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

Failure to remediate vulnerabilities increases the risk that threat actors could exploit system weaknesses for malicious purposes.

Recommendation 4:

We recommend that HPN remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during audit fieldwork.

HPN's Response:

"The Plan has remediated the technical vulnerabilities identified by the auditors during the fieldwork portion of this audit. Demonstration of the remediation is being provided as a separate document under separate cover outside this response."

OIG comments:

HPN provided multiple vulnerability scan reports for various operating systems. However, we were unable to determine if the vulnerabilities were remediated because the scans were performed without administrative credentials. Unauthenticated vulnerability scans do not provide detailed patch information. Therefore, please provide the OPM's Healthcare and Insurance Office, Audit Resolution Group with sufficient evidence that the weaknesses we identified have been remediated.

D. Security Event Monitoring and Incident Response

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting.

HPN has an adequate event monitoring program.

Our review of HPN's security event monitoring and incident response programs identified the following controls in place:

- Policies and procedures for security event monitoring;

- Daily security event log review; and
- Documented incident response plan.

Nothing came to our attention to indicate that HPN has not implemented adequate security event monitoring and incident response controls.

E. Configuration Management

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. HPN employs a team of technical personnel who manage system software configuration for the organization. We evaluated HPN's management of the configuration of its computer servers and databases. We observed the following controls in place:

- An adequately documented configuration management policy;
- A documented and approved exception process; and
- An established patch management process.

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

1. Compliance Auditing

HPN has developed and approved security configuration standards that list specific operating system security settings. HPN annually verifies that its systems are compliant through a manual system review process. However, our compliance test revealed that multiple systems have settings that are not in compliance with organization standards.

NIST SP 800-53, Revision 5, states that the organization should "Monitor and control changes to the configuration settings in accordance with organizational policies and procedures."

Infrequent compliance auditing increases the risk that operating systems are not configured appropriately and left undetected could lead to exploitation by threat actors.

Recommendation 5:

We recommend that HPN improve its compliance auditing program to include routine compliance auditing on all operating systems.

HPN's Response:

"The Plan has implemented a process to execute a review on a quarterly basis for all systems and will align with the SOX requirements. The Plan will provide the results of the next scan to the auditors as a separate document under separate cover from this response."

OIG comments:

HPN provided evidence that a tool has been implemented to routinely determine system compliance. The intent of this recommendation has been addressed. No further action is required.

F. Contingency Planning

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

HPN has adequate controls over contingency planning.

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

- Backups of system-level and user-level data contained in information systems;
- Alternate processing site with controls equivalent to the primary site and sufficient resources to transfer and resume operations; and
- Adequately documented contingency plans.

Nothing came to our attention to indicate that HPN has not implemented adequate contingency planning controls.

G. Application Change Control

We evaluated the policies and procedures governing HPN's application development and change control process.

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

- An adequately documented application change control process;
- Configuration changes are adequately documented; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

Nothing came to our attention to indicate that adequate controls have not been implemented over the application change control process.

Appendix

HEALTH PLAN OF NEVADA
A UnitedHealthcare Company

December 17, 2021

Mr. Matthew Antunez

Auditor-In-Charge
Information Systems Audits Group
U.S. Office of Personnel Management
Office of the Inspector General
1900 E Street, N.W.
Washington, DC 20415

RE: Comments to the Draft Audit Report on Audit of the Information Systems General and Application Controls at Health Plan of Nevada, Inc., Report Number 1C-NM-00-21-028

Dear Mr. Antunez:

On October 22, 2021, the United State Office of Personnel Management, Office of the Inspector General ("OPM/OIG") submitted to the Plan a "Draft Report" (1C-NM-00-21-028) ("Draft Report"), detailing the results of the audit of the Information Systems General and Application Controls at Health Plan of Nevada, Inc. ("HPN"), rate code NM, for contract year 2021. Upon submission, OPM/OIG requested the Plan provide comments to the Draft Report.

The Plan appreciates the opportunity to respond to this Draft Report and the willingness of OPM to help resolve the outstanding issues in this audit. The Plan has used its best efforts to obtain all relevant information to respond to the Draft Report's findings and recommendations. This Response will address each issue presented in the Draft Report.

Access Controls

Identification and Authentication

Recommendation 1:

In its Draft Report, the auditors stated *"We recommend that HPN complete its project to require multi-factor authentication in order to access privileged credentials."*

The Plan completed multi-factor authentication on October 26, 2021. Proof of the implementation has been provided as **Attachment 1** to this response. [Attachment 1 – screen shot RSA token authentication for CyberArk login]

Data Center Physical Access Controls

Recommendation 2:

In the Draft Report, the auditors state *"We recommend that HPN implement piggybacking prevention controls at the entrance to its primary data center."*

The plan has updated its Policy to include the process by which employees gain access to the data center and specifically prohibits piggybacking by requiring each person to swipe their badge to gain access to the data center. Proof of the new policy has been provided as **Attachment 2** to this response. [Attachment 2 – updated policy for access to Data Center]

Recommendation 3:

In the Draft Report, the auditors state *"We recommend that HPN implement multifactor authentication at the entrance to its primary data center."*

The Plan has evaluated the best method of multi-factor authentication at the entrance to its primary data center and determined that most effective method is the installation of cypher locks on both external doors to the data center. Additionally, the Plan is updating the security policy to definitively require guest logging with violations of the policy resulting in corrective actions up to an including termination. The target for completion of the installation of the cypher locks is by January 31, 2022.

Network Security

Vulnerability Management

Recommendation 4:

In the Draft Report, the auditors state *"We recommend that HPN remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during the audit fieldwork."*

The Plan has remediated the technical vulnerabilities identified by the auditors during the fieldwork portion of this audit. Demonstration of the remediation is being provided as a separate document under separate cover outside this response.

Configuration Management

Compliance Auditing

Recommendation 5:

In the Draft Report, the auditors state *"We recommend that HPN improve its compliance auditing program to include routine compliance auditing on all operating systems."*

The Plan has implemented a process to execute a review on a quarterly basis for all systems and will align with the SOX requirements. The Plan will provide the results of the next scan to the auditors as a separate document under separate cover from this response.

Conclusion

In conclusion, the Plan has reviewed the recommendations provided by the auditors and has provided documentation that demonstrates that each recommendation has been addressed. Any remediation that was required as a result of the auditors' recommendation has been completed or is in progress with a date certain provided for resolution.

Once you have had an opportunity to review our response and the documentation provided, please contact me if you have any questions or require additional information.

Respectfully,

Keith E. Nygard
Director, Federal Programs
UnitedHealthcare
(702) 477-0179

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:	Toll Free Number:	(877) 499-7295
	Washington Metro Area	(202) 606-2423

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