



**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
American Postal Workers Union Health Plan**

Report Number 2022-ISAG-0024

February 27, 2023

Executive Summary

Audit of the Information Systems General and Application Controls at American Postal Workers Union Health Plan

Report No. 2022-ISAG-0024

February 27, 2023

Why Did We Conduct the Audit?

The American Postal Workers Union Health Plan (APWUHP) 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 APWUHP's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by APWUHP to process and store data related to medical encounters and insurance claims for FEHBP members as of July 2022.



Michael R. Esser

Assistant Inspector General for Audits

What Did We Find?

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

- As a result of our audit, APWUHP addressed risks it had identified and conducts ongoing vendor risk assessments.
- APWUHP has adequate physical and logical access controls in place.
- APWUHP has not performed adequate vulnerability scans for all assets in its IT environment. Additionally, systems were found with technical weaknesses, some with known exploits.
- APWUHP does not have adequate controls in place related to internal network segmentation and reviewing audit logs.
- APWUHP has not developed baseline or security configuration settings for all operating systems. Additionally, APWUHP does not have a process in place to monitor security configurations.
- As a result of our audit, APWUHP implemented controls related to testing environments, software management, and assessing impacts for IT-related changes.
- As a result of our audit, APWUHP developed business area recovery metrics and conducted an incident response test. However, it does not have sufficient controls in place for event monitoring. Furthermore, adequate vulnerability scanning is not conducted at the backup data center.
- APWUHP does not have adequate controls in place related to developer security standards and training.

Abbreviations

APWUHP	American Postal Workers Union Health Plan
BIA	Business Impact Analysis
CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
IT	Information Technology
MSP	Managed Service Provider
MTD	Maximum Tolerable Downtime
NIST SP	National Institute of Standards and Technology's Special Publication
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	Service Acquisition
SDLC	Software Development Life Cycle
VLAN	Virtual Local Area Network

Table of Contents

Executive Summary	i
Abbreviations	ii
I. Background	1
II. Objectives, Scope, and Methodology	2
III. Audit Findings and Recommendations	4
A. Security Management	4
1. Ongoing Vendor Risk Assessments	4
2. Risk Response	5
B. Access Controls	6
C. Network Security	7
1. Reviewing Scan Reports	7
2. Scan Configuration.....	8
3. Vulnerabilities Identified by OIG Scans	10
4. Firewall Ruleset Review	11
5. Network Segmentation	12
D. Security Event Monitoring and Incident Response	13
1. Audit Log Review	13
2. Incident Response Testing	14
E. Configuration Management	15
1. Baseline Configurations	15
2. Security Configuration Settings	16
3. System Configuration Review	17
4. Impact Analysis.....	18

Table of Contents (Cont.)

5. Software Management.....	18
6. Separate Test Environment	20
F. Contingency Planning.....	21
1. Recovery Metrics	21
2. Disaster Recovery Site Security Controls	22
G. Application Change Control	23
1. Software Development Security Standards.....	24
2. Software Development Process.....	25
3. Software Security Testing and Evaluation	26

Appendix: American Postal Workers Union Health Plan’s January 3, 2023,
response to the draft audit report issued September 21, 2022

Report Fraud, Waste, and Mismangement

I. Background

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by the American Postal Workers Union Health Plan (APWUHP), plan code 47.

The audit was conducted pursuant to FEHBP contract CS 1370; 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.

This was our third audit of the information technology (IT) general and application controls at APWUHP. The previous audits of general and application controls at APWUHP were conducted in 2011 and 2018. Final Audit Report No. 1B-47-00-11-044 was issued on June 27, 2011, and Final Audit Report No. 1B-47-00-17-018 was issued on January 16, 2018. All recommendations from the previous audits have been closed.

All APWUHP 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 APWUHP'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 APWUHP'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 APWUHP's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of APWUHP'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 APWUHP to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Glen Burnie, Maryland.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general and application controls in place over APWUHP'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 APWUHP as of July 2022.

In conducting our audit, we relied to varying degrees on computer-generated data provided by APWUHP. 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 APWUHP's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's Federal Information System Controls Audit Manual;
- Gathered documentation and conducted interviews;
- Reviewed APWUHP'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 to evaluate APWUHP's control structure. These criteria included, but were not limited to, the following publications:

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-39, Managing Information Security Risk; and
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy.

Compliance with Laws and Regulations

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

As a result of this audit, APWUHP addressed the ongoing vendor risk and risk response issues identified and recommendations made.

We observed the following controls in place:

- An adequate IT security awareness training program;
- An adequate initial vendor risk assessment; and
- A documented risk management policy that establishes purpose, scope, roles and responsibilities.

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

1. Ongoing Vendor Risk Assessments

APWUHP utilizes approximately 20 vendors for various business functions. Before a business relationship is entered into with a potential vendor, APWUHP assesses risk through a security questionnaire. If the risk is acceptable, a business relationship can be established. However, APWUHP does not require or perform ongoing vendor risk assessments to evaluate changes in the vendor's security posture.

NIST SP 800-53, Revision 5, control SR-6 advises that the organization should "Assess and review the supply chain-related risks associated with suppliers or contractors"

Additionally, NIST SP 800-53, Revision 5, control RA-3 states that "Risk assessments ... consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities."

Failure to conduct ongoing vendor risk assessments increases the risk that vendors have vulnerabilities outside APWUHP's risk appetite.

Recommendation 1:

We recommend that APWUHP update its policies and procedures and implement a process to conduct ongoing vendor risk assessments.

APWUHP's Response:

“APWUHP has added [REDACTED], as a platform, for the purpose of Vendor Risk Management. This platform allows APWUHP to submit assessments to vendors, based on calculated risk scoring, developed by APWUHP.

On November 17th, APWUHP completed this implementation by issuing its first round of assessments to critical and high graded vendors. Assessments will be sent annually to vendors with critical and high ratings within the [REDACTED] platform. APWUHP submitted evidence to include screen shots from the new portal, an extracted report showing vendors which have received assessments, and the modified policy which requires an annual risk assessment submitted to our vendors.”

OIG Comments:

In response to the draft report, we received sufficient evidence that demonstrates the intent of the recommendation has been met. No further action is required.

2. Risk Response

APWUHP has not responded to all its identified risks. APWUHP's *IT Risk Management Policy* states that risk remediation efforts are addressed through projects. Additionally, APWUHP's *IT Configuration Management Policy* states that patch and update exception requests must be provided to IT management for review and approval. We were provided evidence demonstrating that some identified risks are tracked. However, these risks have not been formally accepted nor have remediation projects been created.

NIST SP 800-53, Revision 5, control RA-7 states that the organization should “Respond to findings from security and privacy assessments, monitoring, and audits in accordance with ... risk tolerance.” Responding to risk includes mitigating, accepting, sharing, or avoiding risk.

Furthermore, NIST SP 800-39 states that “Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance.”

NIST SP 800-39 states that “Explicit understanding and acceptance of the risk to an organization's operations and assets, individuals, other organizations ... by senior leaders/executives (reflecting the organization's risk tolerance) are made in accordance with the organization's risk management strategy... .”

Failure to address risks increases the risk that vulnerabilities remain in the environment beyond tolerance limits of the organization.

Recommendation 2:

We recommend that APWUHP formally respond, document, and track risks in accordance with its policies and procedures.

APWUHP’s Response:

“APWUHP has developed, in accordance with its risk management policy, procedures which address multiple areas of identified risk to the organization. In response to the OIG audit recommendation, APWUHP has provided an updated risk register. This document cataloged identified risks and remediation efforts to address those identified risks.

Within its response, APWUHP has provided the updated document and corresponding evidence, showing the progress made in mitigating these identified risks. Some of the areas include:

- *Risk review and response procedures for end of life systems*
- *Development and implementation of a Risk Identification and Acceptance workflow*
- *Asset identification and configuration management*
- *Updated procedures for account termination*
- *Enhanced reporting for access and account activity*
- *Updated security policies, including modified procedures and logging”*

OIG Comments:

In response to the draft report, we received sufficient evidence that demonstrates the intent of the recommendation has been met. 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 at APWUHP’s headquarters facility and data centers. We also examined the logical access controls

APWUHP has adequate logical and physical access controls in place.

protecting sensitive data on APWUHP's network environment and applications.

We observed the following controls in place:

- Policies and procedures to review and update physical and environmental controls;
- Adequate maintenance of visitor access records; and
- Policies and procedures for granting, removing, and adjusting system and application access.

Nothing came to our attention to indicate that APWUHP has not implemented adequate access controls.

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 APWUHP'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.

APWUHP is working to correct a vulnerability with a known exploit in its IT environment.

We observed the following controls in place:

- Perimeter controls to secure connections to external networks;
- Malicious code protection on end user devices; and
- Adequate network access controls to prevent non-company devices from connecting to the network.

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

1. Reviewing Scan Reports

APWUHP contracts with a managed service provider (MSP) to perform its vulnerability scanning functions. The MSP only scans some APWUHP systems for vulnerabilities and then sends a report of the scan results to APWUHP. The APWUHP *IT Vulnerability Management Policy* states that APWUHP system administrators are required to review the reports and establish remediation plans. However, during our vulnerability scan exercise we discovered that an insufficient account was used to authenticate to some

systems during the exercise. Further, we learned that the insufficient account was used in previous scans unrelated to this audit. Once the account was corrected, our scan exercise yielded many vulnerabilities previously undetected by APWUHP and its MSP. Further, multiple systems were infected with a vulnerability that is listed in the Cybersecurity & Infrastructure Security Agency's known exploited vulnerabilities catalog. We communicated the severity of the vulnerability and APWUHP has committed to remediating the vulnerability in a timely manner.

NIST SP 800-53, Revision 5, control RA-5 states that the organization should "Analyze vulnerability scan reports and results from vulnerability monitoring"

Failure to sufficiently analyze vulnerability scan reports increases the risk that vulnerabilities remain in the environment beyond organizational tolerance limits.

Recommendation 3:

We recommend that APWUHP implement a process to routinely review vulnerability scan reports to ensure thorough scans were performed.

APWUHP's Response:

"No further action required, based off of our last discussion."

OIG Comments:

In response to the draft report, we received evidence that APWUHP updated its *IT Vulnerability Management Policy*. The updates require IT Management to verify that successful scans were performed. Additionally, vulnerability scan reports include a section to report credential errors. No further action is required.

2. Scan Configuration

APWUHP's vulnerability scans are not adequately configured. APWUHP's *IT Vulnerability Management Policy* states that vulnerability scans will be performed on all live network assets that are deployed. However, the systems at the back-up data center are not included in vulnerability scans. Further, we were told that credentials are used to authenticate the vulnerability scans. However, during our vulnerability scan exercise, the MSP reported that credentialed vulnerability scans are not performed on APWUHP's entire range of operating systems.

NIST SP 800-53, Revision 5, control RA-5 states that the organization "Monitor and scan for vulnerabilities in the system and hosted applications"

Additionally, NIST SP 800-53, Revision 5, control RA-5 (5) states that the organization should implement privileged access authorization for vulnerability scanning activities.

Failure to adequately configure vulnerability scans increases the risk that vulnerabilities go undetected.

Recommendation 4:

We recommend that APWUHP perform vulnerability scans on all network assets in accordance with its policy.

APWUHP's Response:

“In response to the proposed recommendation, APWUHP updated its policies and procedures for scanning and addressing vulnerabilities within the APWUHP environment. APWUHP has implemented full credentialed scanning for all systems within its environment and has worked with our security vendor to insure [sic] that reporting is being performed as part of the monthly vulnerability scan. Within this reporting, any errors logged when using provided credentials are presented and a remediation plan will be executed, to include additional scanning.

As part of our response documentation, APWUHP has included log files and screen shots from vulnerability reports, including full scan data which shows access used within vulnerability scanning by privileged accounts on both Windows and non-windows systems. This reporting also includes scans for Disaster Recover (DR) systems at the APWUHP's remote location.

APWUHP has also provided updated IT Security Policies, which reflect the changes in credentialed scanning and outlines the procedures to be taken.”

OIG Comments:

We acknowledge that APWUHP has updated its policy. However, recent APWUHP vulnerability scans show that multiple systems failed to provide results due to inadequate credentials. We recommend that APWUHP continue to work on remediating credentialing issues so that it can perform thorough vulnerability scans on all network assets in accordance with its policy.

Recommendation 5:

We recommend that APWUHP update its policies and procedures and implement a process to perform credentialed scanning on all operating systems.

APWUHP’s Response:

“No further action required, based off of our last discussion.”

OIG Comments:

In response to the draft report, we received evidence that APWUHP updated its *IT Vulnerability Management Policy*. The policy requires IT Management to conduct network mapping scans, that will help to ensure all assets are identified and scanned. No further action is required.

3. Vulnerabilities Identified by OIG Scans

APWUHP’s MSP conducted credentialed vulnerability scans on a sample of servers and workstations in its network environment on our behalf. We chose a sample of 141 servers from a universe of approximately 170. The sample selection 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, as well as other systems in the same general control environment that contain 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 we identified were provided to APWUHP in the form of an audit inquiry. APWUHP was aware of some of the vulnerabilities and has provided plans to address the vulnerabilities that were detected.

NIST SP 800-53, Revision 5, control RA-5 states that organizations should monitor, scan, and remediate legitimate vulnerabilities.

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

Recommendation 6:

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

APWUHP’s Response:

“APWUHP has verified vulnerability scanning across its environment. Through enhancing credentialed scanning and updat[ing] its policies and procedures, APWUHP continues to address known vulnerabilities as they are discovered.”

As part of our audit, APWUHP created a targeted Vulnerability Response Work plan, which has been used to provide evidence of progress made in addressing listed vulnerabilities. APWUHP continues to address vulnerabilities through application remediation, and system replacement/deprecation.”

OIG Comments:

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

4. Firewall Ruleset Review

APWUHP does not routinely review firewall rulesets. In response to this audit finding, APWUHP developed its *IT Firewall Policy* that requires configurations and rulesets to be formally reviewed annually, at a minimum. APWUHP provided evidence that firewall compliance checks are routinely reviewed, however firewall rulesets are not tested or reviewed for necessity or other organizational compliance requirements.

NIST SP 800-41, Revision 1, states that firewall “ruleset reviews or tests [should] be performed periodically to ensure compliance with the organization’s policies.”

Failure to perform firewall ruleset reviews increases the risk that unused or unnecessary rulesets are in place which may increase the risk of an attack.

Recommendation 7:

We recommend that APWUHP develop procedures and implement a process to routinely review firewall rulesets and take corrective actions.

APWUHP’s Response:

“In response to the proposed recommendation, APWUHP has updated its IT Security Policy to include regular scheduled review of firewall rulesets and auditing of configuration. The IT policy also has been updated to include a log sheet, to be completed after each firewall ruleset review. The log includes the date of the review, the technician responsible, notes about findings from the review, and an area to log any change request tickets associated with the review. APWUHP has also created a firewall review checklist, which details those items which should be reviewed, in accordance to the stated policy.

APWUHP has submitted evidence, including the updated IT Security Policy, and log sheets, along with the firewall review checklist.”

OIG Comments:

In response to the draft report, we received sufficient evidence that demonstrates the intent of the recommendation has been met. No further action is required.

5. Network Segmentation

APWUHP does not use firewalls to segment user-controlled systems from sensitive internal resources. APWUHP uses a firewall to control connections with systems outside of its network as well as between public facing applications and the internal network. However, logical segmentation within the internal network between users and sensitive resources is only achieved with virtual local area networks. APWUHP is aware of the gap and has provided a statement of work to address internal network segmentation.

NIST SP 800-41, Revision 1, states that “Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised external attackers. Important internal systems should be placed behind internal firewalls.”

Failure to appropriately separate user-controlled systems from sensitive internal resources increases the risk that a compromise of a user’s system could allow access to sensitive servers and data.

Recommendation 8:

We recommend that APWUHP complete its project to segregate its internal network in order to separate sensitive resources from user-controlled systems.

APWUHP’s Response:

“APWUHP has an approved Statement of Work (SOW) and project plan, with an approved vendor to implement [REDACTED] across our [REDACTED] networks. This is being performed to enhance current network segmentation that APWUHP employs within its core network. With the completion of this network virtualization platform upgrade and implementation, APWUHP will have segmentation for all east/west and routable network traffic within its environment.

Phase I of the project has been completed, to include network and appliance upgrades that will facilitate an [REDACTED] replacement. The full completion of this project is currently scheduled for the 1st quarter of 2023.”

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.

APWUHP does not review audit logs from all operating systems.

We observed the following controls in place:

- Controls to monitor security events throughout the primary data center;
- Policies and standards for analyzing security events; and
- A policy that outlines content of audit records.

However, we noted the following opportunities for improvement related to APWUHP's security event monitoring and incident response controls.

1. Audit Log Review

In addition to scanning for vulnerabilities, APWUHP's MSP also provides a managed detection and response service. Audit logs from the intrusion detection and prevention system are ingested into the MSP's security information and event monitoring tool for threat analysis. Separately, APWUHP utilizes a tool to review audit logs from one type of operating system. However, we did not see evidence that logs from the entire range of operating systems in its IT environment are routinely reviewed.

NIST SP 800-53, Revision 5, control AU-6 states that the organization should review and analyze system audit records for indications of unusual activity at an organization defined frequency.

Failure to review audit logs increases the risk that unwanted or unusual system activity goes undetected.

Recommendation 9:

We recommend that APWUHP update its policies and procedures to include a process to review audit logs from all operating systems in its IT environment.

APWUHP’s Response:

“APWUHP has updated IT Policies and Procedures, requiring all business critical systems, including windows and non-windows systems, have logging shipped to our SEIM appliance. This appliance is managed by the APWUHP security vendor, and is subject to all monitoring and alerting.

Enhanced reporting and alerting, being managed by the APWUHP security vendor has been tested and results have been provided as part of our submission documentation. Along with this information, APWUHP has submitted the updated IT Security policy, along with log files from our security appliance, and screen shots of systems which have been added.”

OIG Comments:

We acknowledge that APWUHP updated its policy. However, the evidence submitted states that work remains to set up log forwarding for multiple operating systems. Once the process to review audit logs from all operating systems in its IT environment has been completed, we recommend that APWUHP submit evidence to OPM Audit Resolution. Sufficient evidence includes screenshots of tools used, reporting features, and log sources.

2. Incident Response Testing

APWUHP has not tested its incident response plan since at least May 2019. APWUHP’s *Policy on Security Incident Procedures* states that incident response training and testing will be conducted on an annual basis. We were told that incident response testing is conducted in combination with disaster recovery tests. However, we reviewed APWUHP’s disaster recovery test results from 2019 through 2021 and determined that incident response testing was not a test objective.

NIST SP 800-53, Revision 5, control IR-3 states that the organization should periodically “Test the effectiveness of the incident response capability”

Failure to conduct incident response testing increases the risk that incident response procedures have weaknesses and deficiencies that may prolong incidents.

Recommendation 10:

We recommend that APWUHP conduct routine incident response testing in accordance with its policy.

APWUHP’s Response:

“No further action required, based off of our last discussion.”

OIG Comments:

In response to the draft report, we received evidence that APWUHP conducted an adequate incident response tabletop exercise and recorded detailed findings in an after-action report. No further action is required.

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. APWUHP employs a team of technical personnel who manage system software configuration for the organization.

APWUHP utilizes operating systems that are no longer supported by the vendor.

We observed the following controls in place:

- Documented configuration management policy;
- Documented system configuration change decisions; and
- Documented policy defining restrictions on the use and installation of software.

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

1. Baseline Configurations

APWUHP has not developed and documented baseline configurations for all systems in its IT environment. APWUHP provided evidence demonstrating that baseline configurations are utilized in some instances. However, multiple systems and operating systems in production do not have baseline configurations.

NIST SP 800-53, Revision 5, control CM-2 states that the organization should “Develop, document, and maintain under configuration control, a current baseline configuration of the system”

Additionally, NIST SP 800-53, Revision 5 states that “Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components,

network topology, and logical placement of components in the system architecture.”

Failure to develop and document baseline configurations for all systems increases the risk that systems will not be securely configured.

Recommendation 11:

We recommend that APWUHP develop, document, and maintain under configuration control, a current baseline configuration for all systems in its IT environment.

APWUHP’s Response:

“APWUHP has approved an application upgrade to implement compliance based configuration management across our environment. This upgrade will pair with current asset management and configuration reporting in use by APWUHP. The upgrade will allow for all systems within the environment to be managed based on compliance level configuration. With the completion of this enhancement, APWUHP will be able to use DISA STIG baselines across all critical business systems.

Phase I of the project is complete, the full completion of this project is 1st quarter of 2023.”

2. Security Configuration Settings

APWUHP has not established and documented configuration settings for all systems which reflect the most restrictive mode consistent with operational requirements. APWUHP utilizes system build guides and a tool to implement parameters that impact the security and privacy posture of some of its systems. However, APWUHP does not have an established process for a variety of other systems in its IT environment.

NIST SP 800-53, Revision 5, control CM-2 states that the organization should “Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements”

Failure to adequately document configuration settings could lead to insufficient or inconsistently applied security and privacy configurations.

Recommendation 12:

We recommend that APWUHP establish and document configuration settings for all systems which reflect the most restrictive mode consistent with operational requirements.

APWUHP’s Response:

“APWUHP has approved an application upgrade to implement compliance based configuration management across our environment. This upgrade will pair with current asset management and configuration reporting in use by APWUHP. The upgrade will allow for all systems within the environment to be managed based on compliance level configuration. With the completion of this enhancement, APWUHP will be able to use DISA STIG baselines across all critical business systems.

Phase I of the project is complete, the full completion of this project is 1st quarter of 2023.”

3. System Configuration Review

APWUHP does not routinely review configuration changes to its systems. Configuration scanning is performed during the initial build process but not routinely thereafter. APWUHP stated that it does not currently have a system in place to monitor configuration changes but intends to investigate and implement a configuration management solution.

NIST SP 800-53, Revision 5, control CM-3 (7) states that the organization should review changes to the system routinely or under organization-defined circumstances to determine whether unauthorized changes have occurred.

Failure to routinely review system changes increases the risk that unauthorized or insecure system configurations will go undetected, leaving the system vulnerable to attack.

Recommendation 13:

We recommend that APWUHP implement a process to review configuration changes to the system routinely or under organization-defined circumstances to determine whether unauthorized changes have occurred. Note – this recommendation cannot be implemented until the controls from Recommendation 12 are in place.

APWUHP’s Response:

“APWUHP has approved an application upgrade to implement compliance based configuration management across our environment. This upgrade will pair with current asset management and configuration reporting in use by APWUHP. The upgrade will allow for all systems within the environment to be managed based on compliance level configuration. With the completion of this enhancement, APWUHP will be able to use DISA STIG baselines across all critical business systems.

Phase I of the project is complete, the full completion of this project is 1st quarter of 2023.”

4. Impact Analysis

APWUHP does not perform security and privacy impact analyses during the change management process. APWUHP’s *IT Change Management Policy* requires all requests for change to be accompanied with a subjective change risk assessment. However, we did not receive evidence of risk assessments for multiple changes we reviewed.

NIST SP 800-53, Revision 5, control CM-4 states that the organization should “Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.”

Failure to perform impact analyses prior to change implementation negatively impacts the organization’s ability to understand and respond to the risks associated with changes.

Recommendation 14:

We recommend that APWUHP analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

APWUHP’s Response:

“No further action required, based off of our last discussion.”

OIG Comments:

In response to the draft report, we received evidence of an IT change request and associated documentation that showed APWUHP analyzed security impact. No further action is required.

5. Software Management

During our vulnerability scanning exercise, numerous instances of unsupported software were identified in APWUHP’s IT environment. In response to our audit finding, APWUHP updated its *IT Vulnerability Management Policy* to describe its methods for addressing unsupported software. It is APWUHP’s policy to monitor the lifecycle of software and extend support. If support is no longer available, system administrators must submit an exception request to management. However, we did not receive evidence that end-of-life software exceptions are in place for any instance of unsupported software in APWUHP’s IT environment.

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

Additionally, NIST SP 800-53, Revision 5, control SA-1 states that the organization should develop and document “Procedures to facilitate the implementation of the system and services acquisition [(SA)] policy and the associated [SA] controls,” which includes the requirements of SA-22.

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

Recommendation 15:

We recommend that APWUHP develop and document policies and procedures which define how unsupported software should be replaced beyond the end-of-life date.

APWUHP’s Response:

“No further action required, based off of our last discussion.”

OIG Comments:

In response to the draft report, we received evidence that APWUHP updated its *IT Vulnerability Management Policy* to define end-of-life software expectations and procedures. No further action is required.

Recommendation 16:

We recommend that APWUHP remove or acquire extended support for all unsupported software in its IT environment.

APWUHP’s Response:

“APWUHP has developed a comprehensive end of life software plan as part of its vulnerability and risk management. Through creation of additional workflow tools, enhanced vulnerability management reporting, and clearly defined policies and procedures, APWUHP is quickly able to identify end of life or end of support systems and applications and respond accordingly.”

APWUHP maintains support on all systems and has used extended support in the past, to allow for production level support on those systems which are being migrated, replaced or removed from its environment.”

OIG Comments:

We acknowledge that APWUHP has updated its policy. However, APWUHP has multiple instances of unsupported software in its environment. We did not receive evidence that all unsupported software was removed, or that extended support licenses were obtained. We continue to recommend that APWUHP remove or identify extended support for all unsupported software in its IT environment.

6. Separate Test Environment

APWUHP does not use a separate test environment to analyze all system changes prior to implementation in an operational environment. APWUHP provided evidence demonstrating a separate test environment is used for some systems. However, they do not have a separate test environment for all systems in its IT environment.

NIST SP 800-53, Revision 5, control CM-4 (1) states that the organization should “analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.”

Failure to analyze system changes in a separate test environment before implementation increases the risk that changes will cause adverse effects that disrupt the business and endanger Federal data.

Recommendation 17:

We recommend that APWUHP use a separate test environment to analyze all system changes prior to implementation in an operational environment.

APWUHP’s Response:

“APWUHP has conducted a review of our server inventory and vulnerability management policies. APWUHP currently has testing systems and procedures designated for all business critical systems.

APWUHP has addressed and satisfies NIST 800-53, R5 by using high availability systems to validate changes before making final changes to all production systems. APWUHP also conducts testing throughout multiple environments prior to release to production systems.

APWUHP has provide[d] updated submission documentation, which includes evidence of updates made to high availability (HA) systems and promoted to production systems through our change management process. APWUHP has also submitted screen shots of test systems which are used for security update and patch testing.”

OIG Comments:

In response to the draft report, we received sufficient evidence that demonstrates the intent of the recommendation has been met. 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 APWUHP's contingency planning documentation and processes to prevent or minimize interruptions to business operations if disruptive events were to occur.

Controls at the disaster recovery site could be improved.

We observed the following controls in place:

- A contingency plan which defines the maintenance of essential business functions during a disruption;
- Routine user-level and system-level data backups; and
- Adequate backup data reliability and integrity testing.

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

1. Recovery Metrics

APWUHP's business impact analysis (BIA) does not contain recovery metrics including maximum tolerable downtime (MTD), recovery time objective (RTO), and recovery point objective (RPO). APWUHP stated that they used to record these metrics, but they are not reflected in the current BIA.

NIST SP 800-53, Revision 5, control CP-2 states that the organization should develop a contingency plan that “provides recovery objectives, restoration priorities, and metrics ...”

Failure to determine and document business area recovery metrics increases the probability that the duration of system outages during an event will be unacceptable to the business.

Recommendation 18:

We recommend that APWUHP perform a business impact analysis that determines and documents recovery metrics including Maximum Tolerable Downtime, Recovery Time Objective, and Recovery Point Objective, for its critical business functions.

APWUHP's Response:

“No further action required, based off of our last discussion.”

OIG Comments:

In response to the draft report, we received evidence of an updated BIA that includes system criticality rankings and return to operation metrics. No further action is required.

2. Disaster Recovery Site Security Controls

APWUHP does not employ alternative mechanisms for security event monitoring, incident response, or vulnerability scanning at the disaster recovery site. At the primary site, security event monitoring, incident response, and vulnerability scanning is performed by APWUHP's MSP. However, the service contract does not include these services for its disaster recovery site. Additionally, we were not provided evidence that APWUHP has coordinated contingency planning with organizational elements responsible for cyber incident response.

NIST SP 800-53, Revision 5, control CP-2 (1) states that the organization should “Coordinate contingency plan development with organizational elements responsible for related plans.” This includes cyber incident response plans.

Additionally, NIST SP 800-53, Revision 5, control CP-13 states that the organization should employ alternative security mechanisms for satisfying security functions when the primary means of implementing the security function is unavailable or compromised.

Failure to implement alternative mechanisms to detect and respond to security events at the disaster recovery site leaves systems and data at the disaster recovery site significantly vulnerable to a cyber-attack.

Recommendation 19:

We recommend that APWUHP coordinate with organizational elements responsible for cyber incident response to implement alternative security mechanisms for security event monitoring, incident response, and vulnerability scanning at the disaster recovery site.

APWUHP’s Response:

“APWUHP has verified with its cybersecurity vendor [Service Provider] that monthly vulnerability scanning includes the VLAN(s) that exist within the Disaster Recovery site. The network expansion has been in place and those systems are part of regular scanning and vulnerability reporting.

APWUHP has submitted updated evidence to include a full scan report, along with updated Disaster Recovery site scan results. This evidence includes windows and non-windows systems, showing complete scans of multiple environments. Additionally, enhanced monitoring and alerting is in place for all environments.”

OIG Comments:

The evidence to demonstrate enhanced monitoring capabilities does not include security-related functions (e.g., operating system event logs, intrusion detection, or firewall logs). Therefore, we are unable to determine if APWUHP has sufficient incident response capabilities at its disaster recovery site. Further, the scan reports that were provided show multiple disaster recovery site systems were unreachable and thus, not scanned for vulnerabilities. We continue to recommend that APWUHP implement security controls detailed above at its disaster recovery site.

G. Application Change Control

We evaluated APWUHP’s application development and change control process. APWUHP primarily utilizes third parties to develop claims processing applications. However, APWUHP does internally develop software to supplement claims system functionality.

APWUHP could improve its SDLC controls.

We observed the following controls in place:

- Documented change management policy;
- Application change review and approval process; and
- Application change documentation tracking.

However, we noted the following opportunities for improvement related to APWUHP’s application change controls.

1. Software Development Security Standards

APWUHP does not train its software developers on organizational standards for building secure software because it has not formally defined policies and procedures for developing secure code.

NIST SP 800-53 Revision 5, control SA-8, states that the organization should apply organization defined systems security and privacy engineering principals, which includes “ensuring that developers are trained on how to develop secure software”

Additionally, NIST SP 800-53, Revision 5, control SA-1 states that the organization should develop and document configuration management policy and “procedures to facilitate the implementation of the system and [SA] policy and the associated [SA] controls,” which includes the requirements of SA-8.

Failure to develop and implement policies and procedures, which define organizational security standards for software development, increases the risk that software will be developed with vulnerabilities.

Recommendation 20:

We recommend that APWUHP develop policies and procedures which define organizational security standards for software development.

APWUHP’s Response:

“APWUHP has built a framework for a comprehensive policy for its Software Development Life cycle standards. In creating this framework, APWUHP will provide a formal policy for all systems (both internal and external) which provide guidelines for best practices in development initiatives within APWUHP. ...

APWUHP expects to have this policy completed and submitted to our QIC for approval in January 2023.”

Recommendation 21:

We recommend that APWUHP train developers on organizational security standards for software development.

APWUHP’s Response:

“APWUHP has obtained a subscription with Pluralsight (<https://app.pluralsight.com>) to provide targeted training for departments within IT. A designated channel has been created for the APPDEV team, in which team members are assigned training courses

and knowledge pathways. We have assigned secure coding training for team members. Through this platform, management will be able to report on completed assignments and create learning programs for developers.

Along with this program, APWUHP will require recertification for the Developer role within the APWUHP APPDEV team, to attest understanding and compliance with the newly crafted SDLC Policy. This re-certification will be required annually and will be accompanied by signed attestation documents by all development staff.

The newly crafted SDLC will be submitted for approval in January 2023.”

2. Software Development Process

APWUHP has not developed a documented software development process. In response to a request for evidence of procedural documentation which defines the software development workflow, APWUHP provided its *IT Change Management Policy*. However, this policy does not define a software development process.

NIST SP 800-53 Revision 5, control SA-15 states that the organization should “Require the developer of the system, system component, or system service to follow a documented development process” Among other things, this documented process must address security and privacy requirements, identify development standards, and document the use of tools.

Failure to document a development process increases the risk that the system development lifecycle will not incorporate sufficient controls to ensure secure software development.

Recommendation 22:

We recommend that APWUHP develop a documented software development process.

APWUHP’s Response:

“APWUHP has built a framework for a comprehensive policy for its Software Development Life cycle standards. In creating this framework, APWUHP will provide a formal policy for all systems (both internal and external) which provide guidelines for best practices in development initiatives within APWUHP. ...

APWUHP expects to have this policy completed and submitted to our QIC for approval in January 2023.”

3. Software Security Testing and Evaluation

APWUHP has not developed and implemented plans for ongoing security and privacy assessments during the system development lifecycle. Therefore, APWUHP does not perform vulnerability analysis and security testing during the software development process.

NIST SP 800-53 Revision 5, control SA-11 states that the organization should “Develop and implement a plan for ongoing security and privacy control assessments”

Additionally, NIST SP 800-53, Revision 5, control SA-11 (2) states that the organization should “Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system”

Finally, NIST SP 800-53, Revision 5, control SA-11 (4) states that the organization should “Require the developer of the system, system component, or system service to perform a manual code review”

Failure to develop and implement a plan for ongoing security and privacy assessments during the system development lifecycle increases the risk that software will be developed with vulnerabilities.

Recommendation 23:

We recommend that APWUHP develop and implement plans for ongoing security and privacy assessments during the system development lifecycle which includes, at a minimum, vulnerability analysis and manual code review.

APWUHP’s Response:

“APWUHP has built a framework for a comprehensive policy for its Software Development Life cycle standards. As part of this policy, we will plan to implement secure code scanning or application secure testing (AST). We have started evaluating this option with an existing platform that we use today. We will be engaging with [REDACTED] to demo their product for our scanning.

APWUHP expects to have this policy completed and submitted to our QIC for approval in January 2023.”

Appendix



American Postal Workers Union Health Plan 2022 OIG Audit Response Section: Draft Report Response

In response to the OIG issued draft report 2022-ISAG-0024 APWUHP Draft Report.pdf, APWUHP is issuing the following response to address recommendations made within the report. APWUHP has issued response documentation, to include evidence which satisfies recommendations made by the OIG audit team. This evidence has included updated policy documents, log files from targeted systems, and screen shots of system activity.

For purposes of organization, APWUHP has crafted responses based on draft report area, section, and recommendation number. Below are the responses to the recommendations, categorized by the areas within the draft report.

A. SECURITY MANAGEMENT

Ongoing Vendor Risk Assessments

OIG Recommendation 1

We recommend that APWUHP update its policies and procedures and implement a process to conduct ongoing vendor risk assessments.

APWUHP Response

APWUHP has added [REDACTED], as a platform, for the purpose of Vendor Risk Management. This platform allows APWUHP to submit assessments to vendors, based on calculated risk scoring, developed by APWUHP.

On November 17th, APWUHP completed this implementation by issuing its first round of assessments to critical and high graded vendors. Assessments will be sent annually to vendors with critical and high ratings within the [REDACTED] platform. APWUHP submitted evidence to include screen shots from the new portal, an extracted report showing vendors which have received assessments, and the modified policy which requires an annual risk assessment submitted to our vendors.

Risk Response

OIG Recommendation 2

We recommend that APWUHP formally respond, document, and track risks in accordance with its policies and procedures.

APWUHP Plan Response

APWUHP has developed, in accordance with its risk management policy, procedures which address multiple areas of identified risk to the organization. In response to the OIG audit recommendation, APWUHP has provided an updated risk register. This document cataloged identified risks and remediation efforts to address those identified risks.

Within its response, APWUHP has provided the updated document and corresponding evidence, showing the progress made in mitigating these identified risks. Some of the areas include:

- Risk review and response procedures for end of life systems
- Development and implementation of a Risk Identification and Acceptance workflow
- Asset identification and configuration management
- Updated procedures for account termination
- Enhanced reporting for access and account activity
- Updated security policies, including modified procedures and logging

B. ACCESS CONTROLS

No recommendation noted.

C. NETWORK SECURITY

Reviewing Scan Reports

No further action required, based off of our last discussion. Scan

Configuration

OIG Recommendation 4

We recommend that APWUHP perform vulnerability scans on all network assets in accordance with its policy.

APWUHP Plan Response

In response to the proposed recommendation, APWUHP updated its policies and procedures for scanning and addressing vulnerabilities within the APWUHP environment. APWUHP has implemented full credentialed scanning for all systems within its environment and has worked with our security vendor to insure [sic] that reporting is being performed as part of the monthly vulnerability scan. Within this reporting, any errors logged when using provided credentials are presented and a remediation plan will be executed, to include additional scanning.

As part of our response documentation, APWUHP has included log files and screen shots from vulnerability reports, including full scan data which shows access used within vulnerability scanning by privileged accounts on both Windows and non-windows systems. This reporting also includes scans for Disaster Recover (DR) systems at the APWUHP's remote location.

APWUHP has also provided updated IT Security Policies, which reflect the changes in credentialed scanning and outlines the procedures to be taken.

OIG Recommendation 5

We recommend that APWUHP update its policies and procedures and implement a process to perform credentialed scanning on all operating systems.

No further action required, based off of our last discussion.

Vulnerabilities Identified by OIG Scans

OIG Recommendation 6

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

APWUHP Plan Response

APWUHP has verified vulnerability scanning across its environment. Through enhancing credentialed scanning and updated its policies and procedures, APWUHP continues to address known vulnerabilities as they are discovered.

As part of our audit, APWUHP created a targeted Vulnerability Response Work plan, which has been used to provide evidence of progress made in addressing listed vulnerabilities.

APWUHP continues to address vulnerabilities through application remediation, and system replacement/deprecation.

Firewall Ruleset Review

OIG Recommendation 7

We recommend that APWUHP develop procedures and implement a process to routinely review firewall rulesets and take corrective actions.

APWUHP Plan Response

In response to the proposed recommendation, APWUHP has updated its IT Security Policy to include regular scheduled review of firewall rulesets and auditing of configuration. The IT policy also has been updated to include a log sheet, to be completed after each firewall ruleset review. The log includes the date of the review, the technician responsible, notes about findings from the review, and an area to log any change request tickets associated with the review. APWUHP has also created a firewall review checklist, which details those items which should be reviewed, in accordance to the stated policy.

APWUHP has submitted evidence, including the updated IT Security Policy, and log sheets, along with the firewall review checklist.

Network Segmentation

OIG Recommendation 8

We recommend that APWUHP complete its project to segregate its internal network in order to separate sensitive resources from user-controlled systems.

APWUHP Plan Response

APWUHP has an approved Statement of Work (SOW) and project plan, with an approved vendor to implement [REDACTED] across our [REDACTED] networks. This is being performed to enhance current network segmentation that APWUHP employs within its core network. With the completion of this network virtualization platform upgrade and implementation, APWUHP will have segmentation for all east/west and routable network traffic within its environment.

Phase I of the project has been completed, to include network and appliance upgrades that will facilitate an [REDACTED] replacement. The full completion of this project is currently scheduled for the 1st quarter of 2023.

D. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Audit Log Review

OIG Recommendation 9

We recommend that APWUHP update its policies and procedures to include a process to review audit logs from all operating systems in its IT environment.

APWUHP Plan Response

APWUHP has updated IT Policies and Procedures, requiring all business critical systems, including windows and non-windows systems, have logging shipped to our SEIM appliance. This appliance is managed by the APWUHP security vendor, and is subject to all monitoring and alerting.

Enhanced reporting and alerting, being managed by the APWUHP security vendor has been tested and results have been provided as part of our submission documentation. Along with this information, APWUHP has submitted the updated IT Security policy, along with log files from our security appliance, and screen shots of systems which have been added.

Incident Response Testing

OIG Recommendation 10

We recommend that APWUHP conduct routine incident response testing in accordance with its policy.

No further action required, based off of our last discussion.

E. CONFIGURATION MANAGEMENT

Baseline Configurations

OIG Recommendation 11

We recommend that APWUHP develop, document, and maintain under configuration control, a current baseline configuration for all systems in its IT environment.

APWUHP Plan Response

APWUHP has approved an application upgrade to implement compliance based configuration management across our environment. This upgrade will pair with current asset management and configuration reporting in use by APWUHP. The upgrade will allow for all systems within the environment to be managed based on compliance level configuration. With the completion of this enhancement, APWUHP will be able to use DISA STIG baselines across all critical business systems.

Phase I of the project is complete, the full completion of this project is 1st quarter of 2023.

Security Configuration Settings

OIG Recommendation 12

We recommend that APWUHP establish and document configuration settings for all systems which reflect the most restrictive mode consistent with operational requirements.

APWUHP Plan Response

APWUHP has approved an application upgrade to implement compliance based configuration management across our environment. This upgrade will pair with current asset management and configuration reporting in use by APWUHP. The upgrade will allow for all systems within the environment to be managed based on compliance level configuration. With the completion of this enhancement, APWUHP will be able to use DISA STIG baselines across all critical business systems.

Phase I of the project is complete, the full completion of this project is 1st quarter of 2023.

System Configuration Review

OIG Recommendation 13

We recommend that APWUHP implement a process to review configuration changes to the system routinely or under organization-defined circumstances to determine whether unauthorized changes have occurred. Note – this recommendation cannot be implemented until the controls from Recommendation 12 are in place.

APWUHP Plan Response

APWUHP has approved an application upgrade to implement compliance based configuration management across our environment. This upgrade will pair with current asset management and configuration reporting in use by APWUHP. The upgrade will allow for all systems within the environment to be managed based on compliance level configuration. With the completion of this enhancement, APWUHP will be able to use DISA STIG baselines across all critical business systems.

Phase I of the project is complete, the full completion of this project is 1st quarter of 2023.

Impact Analysis

OIG Recommendation 14

We recommend that APWUHP analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

No further action required, based off of our last discussion.

Software Management

OIG Recommendation 15

We recommend that APWUHP develop and document policies and procedures which define how unsupported software should be replaced beyond the end-of-life date.

No further action required, based off of our last discussion.

OIG Recommendation 16

We recommend that APWUHP remove or acquire extended support for all unsupported software in its IT environment.

APWUHP Plan Response

APWUHP has developed a comprehensive end of life software plan as part of its vulnerability and risk management. Through creation of additional workflow tools, enhanced vulnerability management reporting, and clearly defined policies and procedures, APWUHP is quickly able to identify end of life or end of support systems and applications and respond accordingly.

APWUHP maintains support on all systems and has used extended support in the past, to allow for production level support on those systems which are being migrated, replaced or removed from its environment.

Separate Test Environment

OIG Recommendation 17

We recommend that APWUHP use a separate test environment to analyze all system changes prior to implementation in an operational environment.

APWUHP Plan Response

APWUHP has conducted a review of our server inventory and vulnerability management policies. APWUHP currently has testing systems and procedures designated for all business critical systems.

APWUHP has addressed and satisfies NIST 800-53, R5 by using high availability systems to validate changes before making final changes to all production systems. APWUHP also conducts testing throughout multiple environments prior to release to production systems.

APWUHP has provide updated submission documentation, which includes evidence of updates made to high availability (HA) systems and promoted to production systems through our change management process. APWUHP has also submitted screen shots of test systems which are used for security update and patch testing.

F. CONTINGENCY PLANNING

Recovery Metrics

OIG Recommendation 18

We recommend that APWUHP perform a BIA that determines and documents recovery metrics including MTD, RTO, and RPO, for its critical business functions.

No further action required, based off of our last discussion.

Disaster Recovery Site Security Controls

OIG Recommendation 19

We recommend that APWUHP coordinate with organizational elements responsible for cyber incident response to implement alternative security mechanisms for security event monitoring, incident response, and vulnerability scanning at the disaster recovery site.

APWUHP Plan Response

APWUHP has verified with its cybersecurity vendor [Service Provider] that monthly vulnerability scanning includes the VLAN(s) that exist within the Disaster Recovery site. The network expansion has been in place and those systems are part of regular scanning and vulnerability reporting.

APWUHP has submitted updated evidence to include a full scan report, along with updated Disaster Recovery site scan results. This evidence includes windows and non-windows systems, showing complete scans of multiple environments. Additionally, enhanced monitoring and alerting is in place for all environments.

G. APPLICATION CHANGE CONTROL

Software Development Security Standards

OIG Recommendation 20

We recommend that APWUHP develop policies and procedures which define organizational security standards for software development.

APWUHP Plan Response

APWUHP has built a framework for a comprehensive policy for its Software Development Life cycle standards. In creating this framework, APWUHP will provide a formal policy for all systems (both internal and external) which provide guidelines for best practices in development initiatives within APWUHP. The focus of this policy highlights the following areas:

- **Planning**
- **Design**
- **Development**
- **Security**
- **Testing**
- **Implementation / Deployment**
- **Review**

APWUHP expects to have this policy completed and submitted to our QIC for approval in January 2023.

OIG Recommendation 21

We recommend that APWUHP train developers on organizational security standards for software development.

APWUHP Plan Response

APWUHP has obtained a subscription with Pluralsight (<https://app.pluralsight.com>) to provide targeted training for departments within IT. A designated channel has been created for the APPDEV team, in which team members are assigned training courses and knowledge pathways. We have assigned secure coding training for team members. Through this platform, management will be able to report on completed assignments and create learning programs for developers.

Along with this program, APWUHP will require recertification for the Developer role within the APWUHP APPDEV team, to attest understanding and compliance with the newly crafted SDLC Policy. This re-certification will be required annually and will be accompanied by signed attestation documents by all development staff.

The newly crafted SDLC will be submitted for approval in January 2023.

Software Development Process

OIG Recommendation 22

We recommend that APWUHP develop a documented software development process.

APWUHP Plan Response

APWUHP has built a framework for a comprehensive policy for its Software Development Life cycle standards. In creating this framework, APWUHP will provide a formal policy for all systems (both internal and external) which provide guidelines for best practices in development initiatives within APWUHP. The focus of this policy highlights the following areas:

- **Planning**
- **Design**
- **Development**
- **Security**
- **Testing**
- **Implementation / Deployment**
- **Review**

APWUHP expects to have this policy completed and submitted to our QIC for approval in January 2023.

Software Security Testing and Evaluation


OIG Recommendation 23

We recommend that APWUHP develop and implement plans for ongoing security and privacy assessments during the system development lifecycle which includes, at a minimum, vulnerability analysis and manual code review.

APWUHP Plan Response

APWUHP has built a framework for a comprehensive policy for its Software Development Life cycle standards. As part of this policy, we will plan to implement secure code scanning or application secure testing (AST). We have started evaluating this option with an existing platform that we use today. We will be engaging with [REDACTED] to demo their product for our scanning.

APWUHP expects to have this policy completed and submitted to our QIC for approval in January 2023.

Name: Matt Grayson
 Title: IT Division Manager (CIO)
 Signature: 
 Date: Jan 3, 2023

Name: Carroll Midgett
 Title: Chief Operating Manager
 Signature: Carroll Midgett
 Date: Jan 3, 2023



Report Fraud, Waste, and Mismanagement

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

By Internet: <https://oig.opm.gov/contact/hotline>

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

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