Memorandum from the Office of the Inspector General

April 29, 2024

Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2023-17434 – CORPORATE WI-FI SECURITY

Attached is the subject final report for your review and management decision. Your written comments, which addressed your management decision and actions for one of the seven recommendations, have been incorporated into the report. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions or wish to discuss our findings, please contact Weston J. Shepherd, Senior Auditor, at (865) 633-7386 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

WJS:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Brett A. Atkins
David W. Baker
Faisal Bhatti
Janda E. Brown
Kenneth C. Carnes II
Sherri R. Collins
Buddy Eller
David B. Fountain
Greg G. Jackson
Joshua Linville
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Dustin C. Pate
John M. Thomas III
Josh Thomas
Ben R. Wagner
OIG File No. 2023-17434

Office of the Inspector General

Audit Report

To the Vice President and Chief Information and Digital Officer, Technology and Innovation

CORPORATE WI-FI SECURITY

Audit Team
Weston J. Shepherd
Scott A. Marler
Brandon P. Roberts

Audit 2023-17434
April 29, 2024

ABBREVIATIONS

NIST	National Institute of Standards and Technology
SPP	Standard Programs and Processes
T&I	Technology and Innovation
TVA	Tennessee Valley Authority
VP	Vice President

TABLE OF CONTENTS

APPENDIX

Audit 2023-17434 – Corporate Wi-Fi Security

EXECUTIVE SUMMARY

Why the OIG Did This Audit

Wi-Fi is the most commonly used wireless communication technology. The Tennessee Valley Authority (TVA) broadcasts multiple Wi-Fi networks at TVA sites for various purposes, such as allowing mobile devices to connect to TVA network resources. Although Wi-Fi provides end users with convenient and widespread network connectivity, TVA's use of Wi-Fi networking increases the risk of unauthorized access,[i] to its network resources. Unauthorized access may be gained through improperly designed or implemented authentication and encryption controls, architecture design gaps, or the presence of unauthorized wireless access points.

Due to the high risks associated with system intrusion and wireless network issues that were identified in a previous audit report,[ii] we performed an audit of TVA's corporate Wi-Fi security controls. Our audit objective was to determine if TVA's security controls were appropriately configured to protect corporate Wi-Fi networks.

What the OIG Found

We determined TVA's security controls related to overall architecture design and implementation were generally configured appropriately to protect corporate Wi-Fi networks. However, we identified several areas that should be addressed to further improve the security of corporate Wi-Fi networks. Specifically, we identified:

- Internal controls for specific types of attacks were ineffective.
- Wireless software and hardware were unsupported by the manufacturer.
- Data in transit (electronic transmission of information) was not properly secured.
- Primary accounts improperly provided privileged user[iii] access.
- Service account[iv] usage was not in accordance with TVA policy.

[i] National Institute of Standards and Technology (NIST) defined unauthorized access as "a person gaining logical or physical access without permission to a network, system, application, data, or other resource."

[ii] Audit Report 2016-15393, *Wireless Local Area Network Deployment*, September 30, 2016.

[iii] NIST defined privileged user as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform."

[iv] TVA defined service accounts as accounts that are used to support an application or software product.

- Baseline configuration management process was not designed or implemented properly.

Specifics of the findings and the corresponding devices and Wi-Fi networks have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on January 22, 2024.

What the OIG Recommends

We made seven recommendations to TVA management to improve internal controls, implement hardware and software updates, and address insecure protocols[v] used to support corporate Wi-Fi networks.

TVA Management's Comments

In response to our draft audit report, TVA management stated they agreed with our recommendations and one of the recommendations had been addressed. See the Appendix for TVA management's complete response.

Auditor's Response

We verified TVA management's actions to address the recommendation have been completed.

[v] NIST defined network protocols as "a set of rules for communications that computers use when sending signals between themselves."

BACKGROUND

Wi-Fi is the most commonly used wireless communication technology. The Tennessee Valley Authority (TVA) broadcasts multiple Wi-Fi networks at TVA sites for various purposes, such as allowing mobile devices to connect to TVA network resources. Although Wi-Fi provides end users with convenient and widespread network connectivity, TVA's use of Wi-Fi networking increases the risk of unauthorized access,[1] to its network resources. Unauthorized access may be gained through improperly designed or implemented authentication and encryption controls, architecture design gaps, or the presence of unauthorized wireless access points.

Organizations can reduce the likelihood of unauthorized access by following best practices for architecture design and implementing security practices, including encryption, configuration management, timely patching, access control, and monitoring. The effectiveness of these practices relies on appropriate design and implementation of security controls.

Due to the high risks associated with system intrusion and wireless network issues that were identified in a previous audit report,[2] we performed an audit of TVA’s corporate Wi-Fi security controls.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if TVA’s security controls were appropriately configured to protect corporate Wi-Fi networks. Our scope was limited to Wi-Fi networks maintained by TVA’s Technology and Innovation (T&I) organization. To achieve our audit objective, we:

- Reviewed applicable TVA Standard Programs and Processes (SPP), including:
  - TVA-SPP-12.704, *Security Configuration Benchmark Standards*
  - TVA-SPP-12.003, *Account Management*
  - TVA-SPP-12.806, *TVA Cybersecurity Patch and Remediation Management Program*
  - TVA-SPP-12.001, *Acceptable Use of Information Resources*
- Performed a walkthrough of network architecture and authentication documentation with TVA personnel to obtain an understanding of the wireless network.
- Reviewed documentation to determine if TVA’s network architecture design aligned with best practices.

[1] National Institute of Standards and Technology (NIST) defined unauthorized access as “a person gaining logical or physical access without permission to a network, system, application, data, or other resource.”

[2] Audit Report 2016-15393, *Wireless Local Area Network Deployment*, September 30, 2016.

- Reviewed a population of 33 wireless network infrastructure devices and gained an understanding of their design and implementation. We then judgmentally selected a risk-based sample of eight unique wireless network devices. For the eight devices, we compared configurations to architecture design for consistency and TVA policy for benchmark standards. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Judgmentally selected 1 of 162 TVA locations with wireless network access. The location was selected based on risk and TVA's wireless architecture design. For the location, we (1) reviewed internal controls designed to prevent unauthorized access to wireless networks and (2) performed walkthroughs to identify any rogue, unknown, or undisclosed devices on property. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Visited two additional TVA locations with wireless network access to identify any rogue, unknown, or undisclosed devices on property. These locations were selected in alignment with other OIG audits being conducted at these locations during fieldwork.
- Reviewed design, implementation, and effectiveness of information system controls associated with TVA's Wi-Fi networks, such as configuration baselines for wireless networks, vulnerability remediation for wireless networks, incident response, and administrative access for devices that manage the wireless networks. We identified these controls as significant to the audit objective and included them in our audit testing.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS

We determined TVA's security controls related to overall architecture design and implementation were generally configured appropriately to protect corporate Wi-Fi networks. However, we identified several areas that should be addressed to further improve the security of corporate Wi-Fi networks. Specifically, we identified:

- Internal controls for specific types of attacks were ineffective.
- Wireless software and hardware were unsupported by the manufacturer.
- Data in transit (electronic transmission of information) was not properly secured.

- Primary accounts improperly provided privileged user[3] access.
- Service account[4] usage was not in accordance with TVA policy.
- Baseline configuration management process was not designed or implemented properly.

Specifics of the findings and the corresponding devices and Wi-Fi networks have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on January 22, 2024.

INTERNAL CONTROLS FOR SPECIFIC TYPES OF ATTACKS WERE INEFFECTIVE

TVA has developed internal controls to prevent, log, detect, and respond to specific types of attacks on wireless networks. We conducted a test and identified weaknesses in TVA's controls to prevent, log, and detect these types of attacks. TVA's response to these activities was not tested due to lack of attack detection. Ineffective controls increase TVA's risk of potential cyber incidents.

WIRELESS SOFTWARE AND HARDWARE WERE UNSUPPORTED BY THE MANUFACTURER

TVA-SPP-12.806, *TVA Cybersecurity Patch and Remediation Management Program,* requires software be supported by the manufacturer. Additionally, end-of-life software must follow a risk evaluation process that includes developing mitigation plans detailing planned actions to update, replace, retire, isolate, or demonstrate other mitigating controls to address out-of-date systems. We reviewed software and hardware versions for two types of wireless network infrastructure devices and determined the majority were unsupported by the manufacturer. Additionally, we determined one type of device had obsolete hardware, which prevents software from being supported by the manufacturer. Table 1 shows the number of devices with unsupported software or hardware.

Equipment Type	Population	Unsupported software	Obsolete hardware
Device type 1	34	32 (94%)	20 (59%)
Device type 2	3277	3254 (99%)	0

Table 1

In addition, mitigation plans have not been developed and documented in accordance with TVA policy. However, there is a planned project in fiscal year 2024 to upgrade the software and hardware. Unsupported hardware and software increase the risk of a potential cyber incidents.

[3] NIST defined privileged user as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform."

[4] TVA-SPP-12.003, *Account Management*, defined service accounts as "accounts that are used to support an application or software product."

DATA IN TRANSIT WAS NOT PROPERLY SECURED

Executive Order 14028, *Improving the Nation's Cybersecurity,*[5] requires encryption for data in transit. During the course of the audit, we identified two insecure protocols[6] with no encryption and weak authentication in use. These two protocols were used for various purposes and have differing levels of risk. The lack of encryption and weak authentication increases TVA's risk of potential cyber incidents.

PRIMARY ACCOUNTS IMPROPERLY PROVIDED PRIVILEGED USER ACCESS

TVA-SPP-12.003, *Account Management,* requires privileged access be separated on a secondary account, rather than a user's primary account. Secondary privileged user accounts have additional controls that increase the accountability of user activity and the security for access controls when compared to primary user accounts. Therefore, primary user accounts should not have privileged access. We reviewed 74 user accounts with privileged access to wireless network infrastructure devices. We identified five primary user accounts with privileged access. Prior to the completion of our audit, TVA T&I took action to address the five primary user accounts with privileged access. Primary user accounts with privileged access was a repeat finding from a previous audit of privileged account management.[7]

SERVICE ACCOUNT USAGE WAS NOT IN ACCORDANCE WITH TVA POLICY

TVA-SPP-12.003, *Account Management*, requires that service account access must be gained through credential escalation procedures and meet TVA minimum password complexity and aging requirements. We identified nine service accounts used for wireless infrastructure that did not utilize credential escalation procedures and did not meet password complexity and aging requirements. Credential escalation procedures and password rules increase the security of service accounts.

[5] United States, Executive Order of the President [Joseph Biden] Compilation of Presidential Documents, Executive Order 14028 - Improving the Nation's Cybersecurity, May 17, 2021, <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>, accessed on January 11, 2024.

[6] NIST defined network protocols as "a set of rules for communications that computers use when sending signals between themselves."

[7] Audit Report 2021-15777, *Privileged Account Management*, September 22, 2021.

BASELINE CONFIGURATION MANAGEMENT PROCESS WAS NOT DESIGNED OR IMPLEMENTED PROPERLY

Configuration management focuses on establishing and maintaining the integrity of devices and has a direct impact on the security posture of systems. We assessed the design, implementation, and effectiveness of the baseline configuration management process and identified several weaknesses. Specifically, we determined (1) there were no requirements in place for periodic baseline configuration reviews, as required by NIST;[8] (2) zero of the eight configurations we reviewed followed documented TVA baselines; and (3) there was no monitoring to ensure wireless network infrastructure devices were in compliance with documented baselines, as required by TVA policy.

In addition, we determined that TVA has documented baseline deviations from best practices. However, TVA has not communicated deviations with Cybersecurity Risk Management to document risks, compensating controls, and impacts, as required by TVA policy.

RECOMMENDATIONS

We recommend the Vice President (VP) and Chief Information and Digital Officer, T&I:

1. Update and implement internal controls to properly defend, detect, and respond to specific types of wireless attacks.

2. Implement the planned project to upgrade software and hardware to supported versions.

3. Take action to remediate both instances of insecure protocols in use where technically and operationally possible.

4. Design and implement a process to identify and remediate primary user accounts that should not be included in privileged access groups.

5. Identify and review service accounts used for wireless infrastructure to ensure all service accounts are appropriately secured where technically and operationally possible.

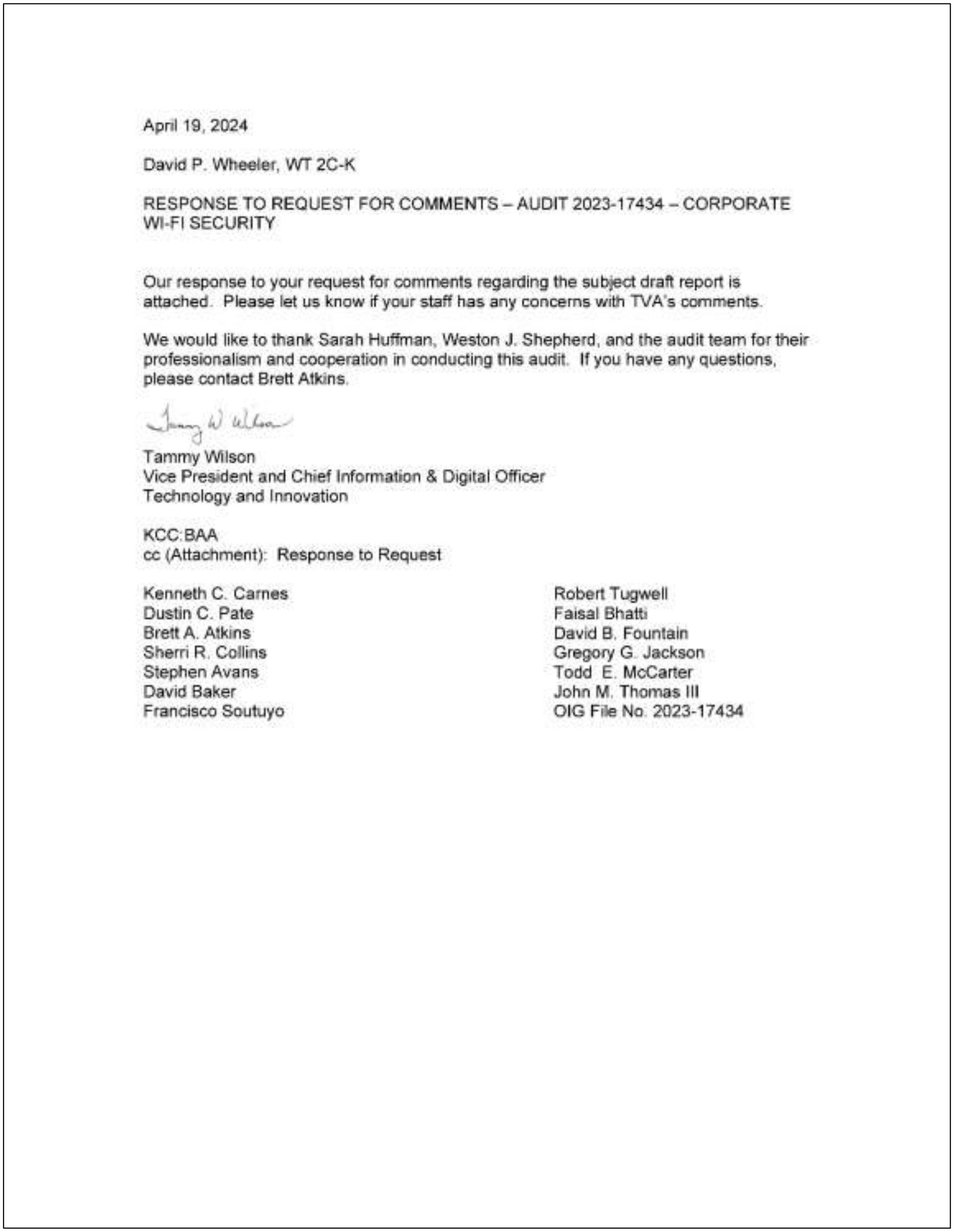
6. Update TVA policy to align with best practice for baseline configuration reviews.

7. Implement baselines, baseline monitoring, and deviation risk tracking as required by TVA policy.

[8] NIST Special Publication 800-53 (Revision 5), Security and Privacy Controls for Information Systems and Organizations, September 2020, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed on 9/26/2023.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendations and took action to address the recommendation regarding updating and implementing controls to respond to specific types of wireless attacks. See the Appendix for TVA management's complete response.

Auditor's Response – We verified TVA management's actions to address the recommendation have been completed.



April 19, 2024

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2023-17434 – CORPORATE WI-FI SECURITY

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Weston J. Shepherd, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.

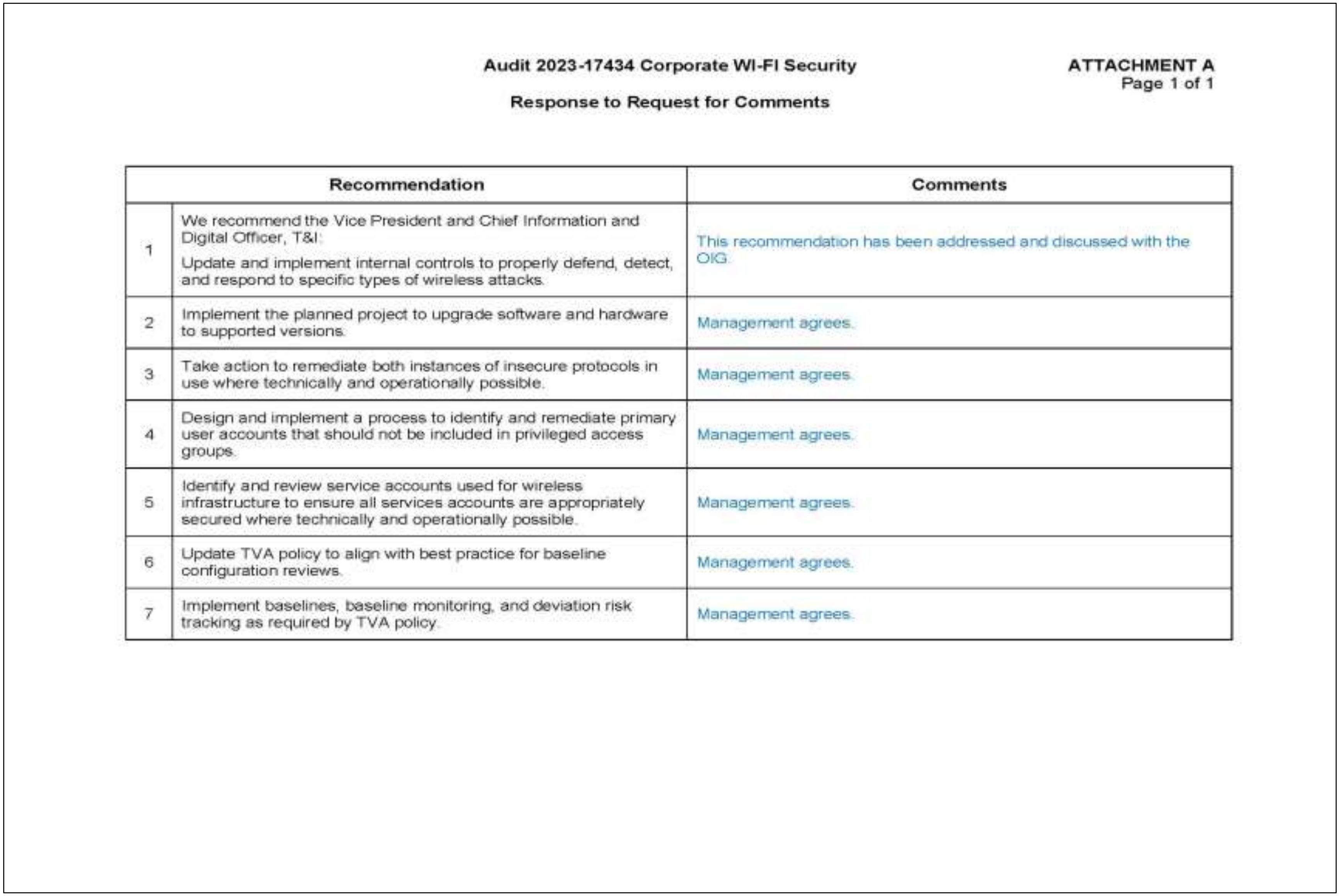
Tammy W Wilson

Tammy Wilson
Vice President and Chief Information & Digital Officer
Technology and Innovation

KCC:BAA
cc (Attachment): Response to Request

Kenneth C. Carnes
Dustin C. Pate
Brett A. Atkins
Sherri R. Collins
Stephen Avans
David Baker
Francisco Soutuyo

Robert Tugwell
Faisal Bhatti
David B. Fountain
Gregory G. Jackson
Todd E. McCarter
John M. Thomas III
OIG File No. 2023-17434



Audit 2023-17434 Corporate WI-FI Security

Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	We recommend the Vice President and Chief Information and Digital Officer, T&I: Update and implement internal controls to properly defend, detect, and respond to specific types of wireless attacks.	This recommendation has been addressed and discussed with the OIG.
2	Implement the planned project to upgrade software and hardware to supported versions.	Management agrees.
3	Take action to remediate both instances of insecure protocols in use where technically and operationally possible.	Management agrees.
4	Design and implement a process to identify and remediate primary user accounts that should not be included in privileged access groups.	Management agrees.
5	Identify and review service accounts used for wireless infrastructure to ensure all services accounts are appropriately secured where technically and operationally possible.	Management agrees.
6	Update TVA policy to align with best practice for baseline configuration reviews.	Management agrees.
7	Implement baselines, baseline monitoring, and deviation risk tracking as required by TVA policy.	Management agrees.