Memorandum from the Office of the Inspector General

May 14, 2024

Allen A. Clare
Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2023-17419 – NETWORK ARCHITECTURE – HYDRO

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 Brandon P. Roberts, Auditor, at (865) 633-7335 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)

BPR: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
Samuel P. Delk
Buddy Eller
David B. Fountain
Greg G. Jackson
Joshua Linville
T. Daniel Lunsford
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Donald A. Moul
Dustin C. Pate
Ronald R. Sanders II
John M. Thomas III
Josh Thomas
Ben R. Wagner
Kay W. Whittenburg
Jacinda B. Woodward
OIG File No. 2023-17419

Office of the Inspector General

Audit Report

To the Senior Vice President, Power Operations, and to the Chief Information and Digital Officer, Technology and Innovation

NETWORK ARCHITECTURE – HYDRO

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

Audit 2023-17419
May 14, 2024

ABBREVIATIONS

NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of the Inspector General
SOP	Standard Operating Procedure
SP	Special Publication
SPP	Standard Programs and Processes
T&I	Technology and Innovation
TVA	Tennessee Valley Authority
WI	Work Instruction

TABLE OF CONTENTS

APPENDIX

Audit 2023-17419 – Network Architecture – Hydro

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Tennessee Valley Authority (TVA) and most modern businesses rely on technology to support business operations. Network architecture has become increasingly important in the design and implementation of complex networks and serves to improve efficiency, scalability, reliability, and resiliency against security threats. Communication and data paths between assets, applications, and other networks are defined in a network's architecture and provide the basis for a business to technologically meet its mission and objectives.

Failure or misconfiguration of TVA's network architecture has the potential to affect critical activities and systems, such as communications, generation control systems, monitoring systems, and business productivity applications. Due to risks associated with misconfigured assets, physical security weaknesses, and technology failure, we performed an audit of the network architecture at a TVA hydroelectric facility. Our objective was to determine if the network architecture and assets in use to support site business and operations were compliant with TVA policies, procedures, and identified best practices.

What the OIG Found

We determined several areas of the network architecture and assets did not follow TVA policies, procedures, or identified best practices. Specifically, we identified the following issues:

- Network redundancy was not implemented in accordance with identified best practices.
- Network asset retirement was not implemented in accordance with Power Operations' Standard Operating Procedures (SOPs).
- Power Operations' location specific SOP did not require unique passwords in accordance with identified best practices.

In addition, we identified the following internal control deficiencies significant to our audit objective:

- Baseline configurations were not implemented in accordance with location specific Power Operations' SOP.
- Physical access permissions and controls were not implemented in accordance with identified best practices.

What the OIG Recommends

We made five recommendations to TVA management to improve network redundancy, remove a retired control network asset, revise procedures, implement a configuration management process, and properly secure and control physical access to all business network assets.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

BACKGROUND

The Tennessee Valley Authority (TVA) and most modern businesses rely on technology to support business operations. Network architecture has become increasingly important in the design and implementation of complex networks and serves to improve efficiency, scalability, reliability, and resiliency against security threats. Communication and data paths between assets, applications, and other networks are defined in a network's architecture and provide the basis for a business to technologically meet its mission and objectives.

Networks provide the communication path between users, processes, applications, and services; TVA relies on these networks for communication, accessing critical applications, and operating its core business functions. TVA locations may utilize multiple networks with differing functions. The network architecture at these locations may include network segmentation to ensure the integrity and confidentiality of information.

Failure or misconfiguration of TVA's network architecture has the potential to affect critical activities and systems, such as communications, generation control systems, monitoring systems, and business productivity applications. Organizations can reduce the likelihood of failed or misconfigured network architectures by following best practices for architecture design and cybersecurity. Due to risks associated with misconfigured assets, physical security weaknesses, and technology failure, we performed an audit of the network architecture at a TVA hydroelectric facility.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if the network architecture and assets in use to support site business and operations were compliant with TVA policies, procedures, and identified best practices. The scope of this audit was limited to a hydroelectric facility with control network assets owned and maintained by TVA's Power Operations organization, and business network and wireless assets owned and maintained by Technology and Innovation (T&I). To achieve our objective, we:

- Identified and reviewed relevant TVA agency-wide and business unit policies, procedures, and Work Instructions (WI) (such as Standard Programs and Processes [SPP] and Standard Operating Procedures [SOP]) to gain an understanding of network architecture and asset processes, including:
  - TVA-SPP-12.008, *Cybersecurity Policy*
  - Information Technology WI-12.405, *Replacement, Redeployment, Storage, Removal & Update of Network Devices*
  - Power Operations' SOP-12.862, *Operational Technology Asset Inventory*
  - Power Operations' location specific SOP

- Reviewed publications and guides to identify applicable best practices, including:
  - National Institute of Standards and Technology (NIST)
    - *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018
    - Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, September 2020
  - Network asset manufacturer's recommendations for a secure environment
  - National Security Agency (NSA) Cybersecurity Technical Report, *Network Infrastructure Security Guide*, October 2023
- Identified and assessed internal controls to the extent necessary to address the audit objective, including:
  - Identified internal controls associated with configuration management, environmental and physical protection, and system and data protection.
  - Assessed design of internal controls by comparing TVA policies, procedures, and WIs to identified best practices.
  - Assessed implementation and operating effectiveness of internal controls by reviewing baseline configurations, physical access permissions, and boundary protection network assets.
- Reviewed network architecture documentation applicable to the hydroelectric facility to perform a network architecture analysis and confirmed our results with TVA personnel.
- Utilized a nonstatistical judgmental approach to select 11 control network assets and three business network assets for a configuration analysis to determine if boundary protection processes and cybersecurity best practices were appropriately implemented. Assets were selected based on their function and potential risk of misconfiguration or failure. Specifics of the population have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity. Since this was not a statistical sample, the results of the sample cannot be projected to the population.
- Conducted interviews with TVA personnel to gain an understanding of the facility's network architecture.
- Performed a walkthrough and observed the hydroelectric facility's layout and network architecture in September 2023.
- Utilized a nonstatistical random approach to sample 15 business network assets and 20 control network assets to perform a network inventory validation. Specifics of the population have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity. Since this was not a statistical sample, the results of the sample cannot be projected to the population.
- Performed a network traffic analysis to determine if boundary protection processes and network segmentation were appropriately implemented.

- Reviewed physical access permissions and controls applicable to network assets at the hydroelectric facility to determine if physical access processes were appropriately implemented.

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 several areas of the network architecture and assets did not follow TVA policies, procedures, or identified best practices. Specifically, we identified the following issues:

- Network redundancy was not implemented in accordance with identified best practices.
- Network asset retirement was not implemented in accordance with Power Operations' SOP.
- Power Operations' location specific SOP did not require unique passwords in accordance with identified best practices.

In addition, we identified the following internal control deficiencies significant to our audit objective:

- Baseline configurations were not implemented in accordance with location specific Power Operations' SOP.
- Physical access permissions and controls were not implemented in accordance with identified best practices.

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

LACK OF NETWORK REDUNDANCY

We performed a network architecture analysis by reviewing network architecture documentation and confirming our understanding of the network architecture during our physical walkthrough and interviews with Power Operations' personnel. We identified several single points of failure[1] that had a potential to impact operations. According to Power Operations' personnel, design changes to address the lack of network redundancy had been submitted prior to our audit. However, the design changes (1) had not been implemented and (2) did not include all single points of failure we identified. Implementing network redundancy as described by the network asset manufacturer would reduce the risk of potential impacts to network availability, generation control, and operations monitoring.

RETIRED NETWORK ASSETS ACTIVE ON CONTROL AND BUSINESS NETWORKS

We performed a physical walkthrough and observation of a sample of 15 business and 20 control network assets and determined that network asset inventory processes were designed according to identified best practices and the sample of 35 assets were appropriately tracked in TVA's inventory; however, we identified two additional active assets during our walkthrough and observation that should have been retired. Maintaining an accurate network inventory allows resources to be efficiently allocated, reduces the likelihood of theft or misuse, assists recovery from operational disruptions, and minimizes security risks due to outdated hardware or unsupported software.

During our walkthrough, we identified a control network asset that according to TVA's record of inventory was "decommissioned." According to Power Operations' personnel, the asset was active and performing network operations. Power Operations' SOP-12.862, *Operational Technology Asset Inventory*, requires a periodic spot check validation of the asset inventory. We determined the retirement process was started; however, the process was never completed to physically remove the asset from service in a timely manner.

In addition, we identified a business network asset that appeared to be in use but should have been retired. According to T&I personnel, the network asset was a retired model and should have been removed from the network. We identified the asset in T&I's inventory and confirmed it had an active network connection. Prior to the completion of our audit, T&I personnel disabled the network asset's connection.

UNIQUE PASSWORDS NOT REQUIRED BY PROCEDURES

Cybersecurity best practices published by the NSA[2] specify the need for unique passwords among assets and privilege levels to reduce the risk of system

[1] A single point of failure within a network refers to a component that, if it fails, creates a domino effect of further failures within a network because other assets and components rely on the single point for functionality.

[2] National Security Agency Cybersecurity Technical Report, *Network Infrastructure Security Guide*, Version 1.2, October 2023.

compromise through password reuse and limit potential pivoting[3] within a network by an attacker. However, we determined that unique passwords for network assets, local accounts, and services were not required by the Power Operations' SOP applicable to the facility. In addition, we reviewed configurations for a selection of 11 control network assets and determined unique passwords were not being utilized.

LACK OF BASELINE CONFIGURATIONS FOR NETWORK ASSETS

The Power Operations' SOP applicable to the facility requires the creation and maintenance of baseline configurations. According to Power Operations' personnel, they have not been capturing baseline configurations for network assets. We compared a selection of 11 control network asset configurations with manufacturer recommendations for a secure environment and identified two configurations that did not follow recommended secure settings.

INAPPROPRIATE PHYSICAL ACCESS TO NETWORK ASSETS

We reviewed physical access at the hydroelectric facility and identified (1) inappropriate physical access permissions to rooms housing business and control network assets and (2) ineffective physical access controls for business network assets. Implementing physical security controls as described in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*,[4] would reduce the risk of inappropriate access, insider threats, damage, and possible theft or data loss.

Inappropriate Physical Access Permissions

We determined that physical access processes were designed according to identified best practices. However, we reviewed physical access permissions and identified 177 individuals with inappropriate access to rooms containing network assets based on their job function. We discussed our finding with Power Operations' management on January 22, 2024, and confirmed the inappropriate physical access. As a result, TVA took action to address the inappropriate physical access permissions.

Ineffective Physical Access Controls

During our physical walkthrough and observation, we identified an unlocked network closet that contained T&I-managed equipment. According to on-site personnel, the closet was always unlocked. In addition, we identified business network assets installed in open areas without proper physical access controls.

[3] Pivoting within a network refers to the act of an attacker moving from one compromised system component to one or more other system components.

[4] 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 1/10/2023.

RECOMMENDATIONS

We recommend the Senior Vice President, Power Operations:

1. Implement planned design changes to address network redundancy and implement additional changes to address single points of failure.

2. Remove the decommissioned asset from the network and follow the operational technology asset inventory validation as required by Power Operations' SOP-12.862, *Operational Technology Asset Inventory*.

3. Revise procedures to require unique passwords for assets, local accounts, and services.

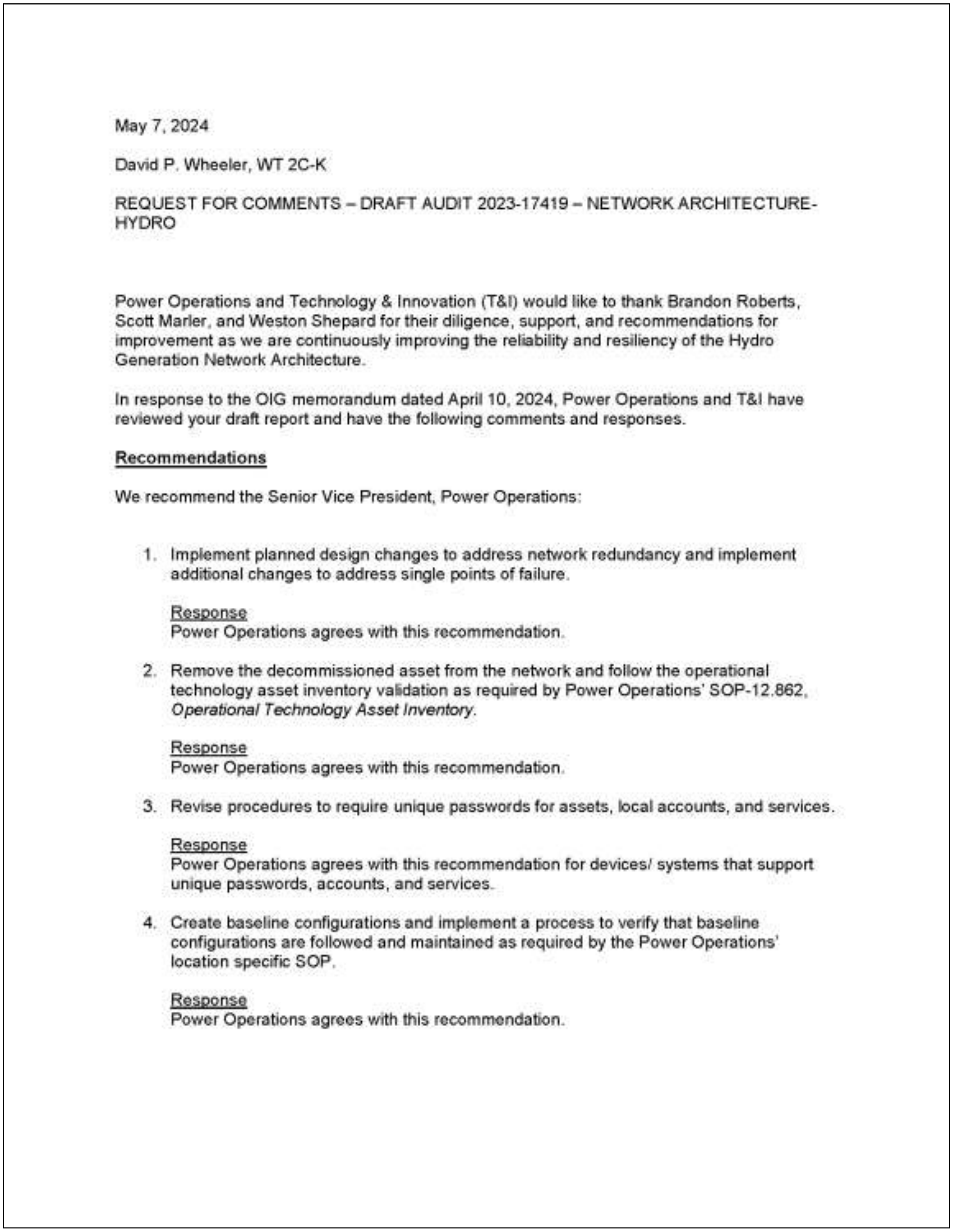
4. Create baseline configurations and implement a process to verify that baseline configurations are followed and maintained as required by the Power Operations' location specific SOP.

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

5. Properly secure and control physical access to all business network assets at the hydroelectric facility in accordance with NIST SP 800-53, Revision 5.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

APPENDIX
Page 1 of 2



May 7, 2024

David P. Wheeler, WT 2C-K

REQUEST FOR COMMENTS – DRAFT AUDIT 2023-17419 – NETWORK ARCHITECTURE-HYDRO

Power Operations and Technology & Innovation (T&I) would like to thank Brandon Roberts, Scott Marler, and Weston Shepard for their diligence, support, and recommendations for improvement as we are continuously improving the reliability and resiliency of the Hydro Generation Network Architecture.

In response to the OIG memorandum dated April 10, 2024, Power Operations and T&I have reviewed your draft report and have the following comments and responses.

Recommendations

We recommend the Senior Vice President, Power Operations:

1. Implement planned design changes to address network redundancy and implement additional changes to address single points of failure.

   Response
   Power Operations agrees with this recommendation.

2. Remove the decommissioned asset from the network and follow the operational technology asset inventory validation as required by Power Operations' SOP-12.862, *Operational Technology Asset Inventory*.

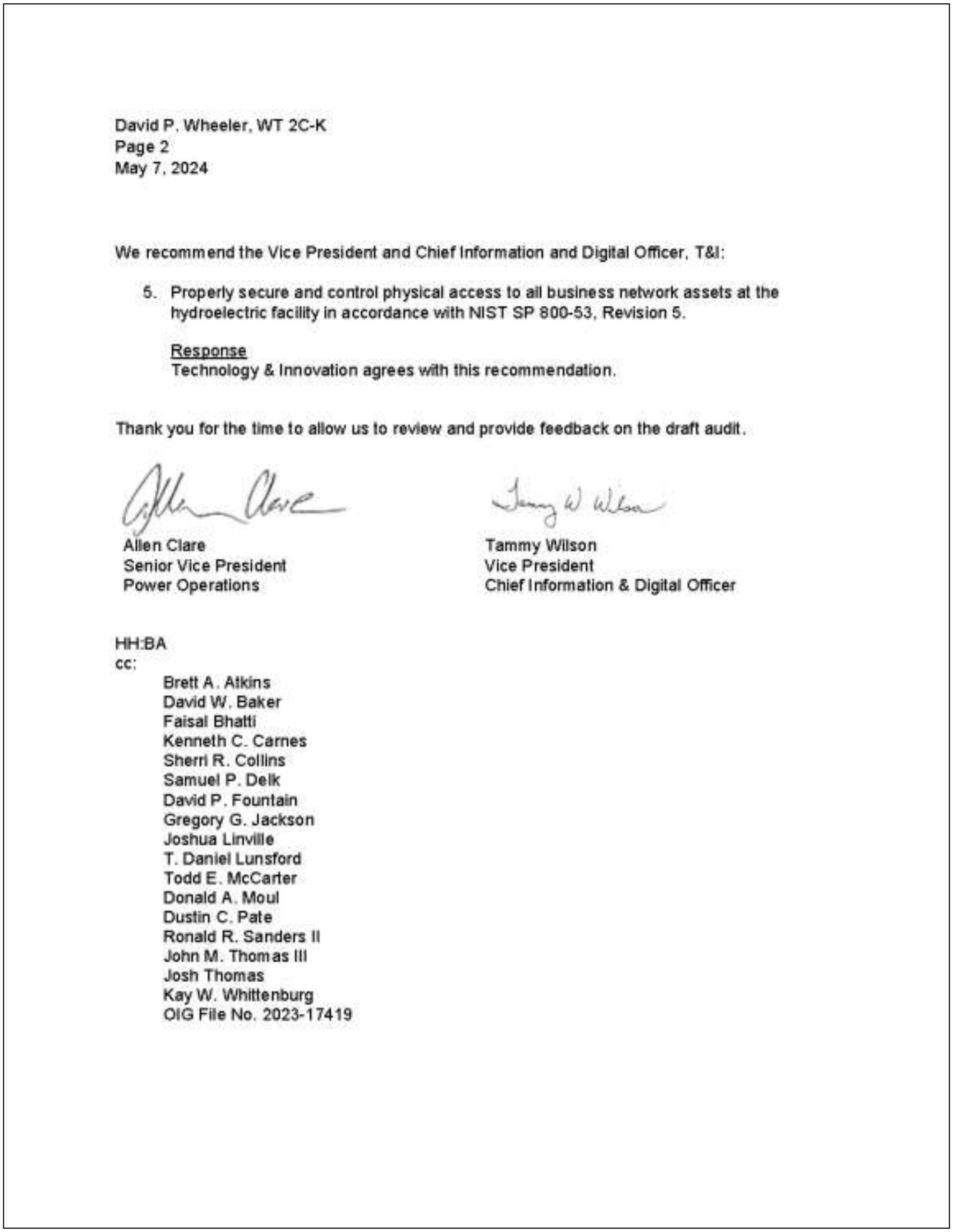
   Response
   Power Operations agrees with this recommendation.

3. Revise procedures to require unique passwords for assets, local accounts, and services.

   Response
   Power Operations agrees with this recommendation for devices/ systems that support unique passwords, accounts, and services.

4. Create baseline configurations and implement a process to verify that baseline configurations are followed and maintained as required by the Power Operations' location specific SOP.

   Response
   Power Operations agrees with this recommendation.



David P. Wheeler, WT 2C-K
Page 2
May 7, 2024

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

5. Properly secure and control physical access to all business network assets at the hydroelectric facility in accordance with NIST SP 800-53, Revision 5.

   Response
   Technology & Innovation agrees with this recommendation.

Thank you for the time to allow us to review and provide feedback on the draft audit.

Allen Clare — Tammy W Wilson

Allen Clare
Senior Vice President
Power Operations

Tammy Wilson
Vice President
Chief Information & Digital Officer

HH:BA
cc:
Brett A. Atkins
David W. Baker
Faisal Bhatti
Kenneth C. Carnes
Sherri R. Collins
Samuel P. Delk
David P. Fountain
Gregory G. Jackson
Joshua Linville
T. Daniel Lunsford
Todd E. McCarter
Donald A. Moul
Dustin C. Pate
Ronald R. Sanders II
John M. Thomas III
Josh Thomas
Kay W. Whittenburg
OIG File No. 2023-17419