Memorandum from the Office of the Inspector General

May 14, 2025

Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2024-17522 – MICROSOFT 365®
ACCESS CONTROL

Due to the importance of proper access control and high-risks associated with improper or misconfigured access control, we audited Microsoft 365® (M365) access control implemented by the Tennessee Valley Authority (TVA) Information Technology (IT) personnel. Our objective was to determine if TVA's corporate deployment of Microsoft 365® is configured to require and enforce the use of multi-factor authentication (MFA) for all accounts.

We determined TVA has required and enforced the use of MFA for all accounts with limited exclusions for service accounts. Additionally, we reviewed a sample of service accounts and determined they were approved and documented in accordance with the applicable tech standard. However, we identified internal control deficiencies related to MFA enforcement access policies and MFA applicability to enterprise applications. Specifically, we found (1) an MFA enforcement access policy applicable to 26 of 2,448 enterprise applications was not fully implemented in accordance with the applicable TVA tech standard and identified best practices, and (2) 1,802 of 2,448 enterprise applications were not covered by an MFA enforcement access policy.

We made four recommendations to TVA management to improve internal controls related to MFA for enterprise applications. In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

BACKGROUND

Microsoft® defines access control as " . . . an essential element of security that determines who is allowed to access certain data, apps, and resources – and in what circumstances."[1] MFA is a type of access control that requires users be verified by more than a single authentication method. Common authentication factors and methods include something you know (e.g., a password), something you have (e.g., an identification badge or cryptographic key), or something you are (e.g., a fingerprint or other biometric data). MFA for Microsoft 365® is managed through Microsoft Entra® ID and supports multiple methods of MFA, including authenticator applications, physical security tokens, biometrics, and certificate-based authentication.

[1] Microsoft®, "What is access control?," <https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control>, accessed on October 3, 2024.

TVA's corporate deployment of Microsoft 365® includes MFA enforcement for both enterprise accounts and applicable enterprise applications. TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*, defines the minimum cybersecurity requirements for the implementation of MFA. In addition, the Office of Management and Budget (OMB)[2] requires MFA for all enterprise accounts.

According to the Cybersecurity and Infrastructure Security Agency (CISA), the use of MFA decreases the likelihood of a successful credential attack by 99 percent. Security is fortified by MFA because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement.

Due to the importance of proper access control and high-risks associated with improper or misconfigured access control, we audited Microsoft 365® access control implemented by TVA IT personnel.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA's corporate deployment of Microsoft 365® is configured to require and enforce the use of MFA for all accounts. The scope of this audit was limited to MFA managed through Microsoft Entra® ID. To achieve our objective, we:

- Identified and reviewed relevant TVA agency-wide policies, procedures, and tech standards to gain an understanding of access control requirements and implementation, including:
  - TVA Standard Programs and Processes 12.003, *Account Management*.
  - TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*.
  - TVA Tech Standard, *Directory Services – Digital Identities of Non-TVA User*.
- Reviewed publications and guides to identify applicable best practices, including:
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, September 2020.
  - NIST SP 800-63B, *Digital Identity Guidelines*, *Authentication and Lifecycle Management*, June 2017.
  - CISA's *Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines,* December 2023.
- Identified internal control to be significant to the audit and performed testing to the extent necessary to address the audit objective. Specifically, we:
  - Identified identification and authentication for organizational and nonorganizational users as key information systems controls.

[2] OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," January 26, 2022, <https://zerotrust.cyber.gov/downloads/M-22-09 Federal Zero Trust Strategy.pdf>, accessed on February 18, 2025.

  - Assessed design of internal controls by reviewing applicable policies, procedures, tech standards, and identified best practices to determine if the controls, as designed, were capable of meeting their intended objectives.
  - Assessed implementation and operating effectiveness of internal controls to determine if access control requirements were properly configured according to applicable policies, procedures, tech standards, and identified best practices.
  - Assessed applicability of MFA to TVA's enterprise applications through review of MFA enforcement access policies to determine if they were configured according to applicable tech standards and identified best practices.

- Inquired of TVA IT personnel to gain an understanding of TVA's implementation of Microsoft 365® and its access control configuration within Microsoft Entra®.
- Reviewed accounts and enterprise applications excluded from access control requirements to verify adherence with applicable policies, procedures, and tech standards.
- Judgmentally selected a sample of 29 excluded service accounts based on most recent creation date and 5 additional that did not appear to follow a common naming convention. The resulting sample totaled 34 service accounts from a population of 288 excluded from MFA as of January 27, 2025. For each sampled account, we confirmed their exclusion was documented as required by the applicable tech standard. Since this was not a statistical sample, the results of the sample cannot be projected to the population.

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 reviewed TVA's Microsoft Entra® ID account listing and performed data analysis against TVA's MFA records to confirm all user accounts were required and enforced to use MFA. We determined TVA has required and enforced the use of MFA for all accounts with limited exclusions for service accounts. Additionally, we reviewed a sample of service accounts and determined they were approved and documented in accordance with the applicable tech standard.

However, we identified internal control deficiencies related to MFA enforcement access policies and MFA applicability to enterprise applications. Specifically, we found (1) an MFA enforcement access policy applicable to 26 of 2,448 enterprise applications was not fully implemented in accordance with the applicable TVA tech standard and identified best practices, and (2) 1,802 of 2,448 enterprise applications were not covered by an MFA enforcement access policy.

Specifics of the findings 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 March 17, 2025.

MFA ENFORCEMENT ACCESS POLICY NOT FULLY IMPLEMENTED IN ACCORDANCE WITH TVA TECH STANDARD

TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*, requires (1) a reauthentication frequency of once every 12 hours and (2) all networks use MFA enforcement. We identified one MFA enforcement access policy applicable to 26 of 2,448 enterprise applications with (1) no defined reauthentication frequency and (2) a network exclusion that allowed enterprise application access without MFA enforcement. A user's presence and identity during an MFA session cannot be verified without a defined reauthentication frequency. In addition, excluding networks from MFA enforcement increases the risk of unauthorized access to information systems.

SUBSET OF ENTERPRISE APPLICATIONS NOT COVERED BY AN MFA ENFORCEMENT ACCESS POLICY

TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*, outlines the process for determining an enterprise application's applicability to MFA enforcement. We identified 1,802 of 2,448 enterprise applications with no associated MFA enforcement access policy. According to TVA personnel, several of the enterprise applications we identified were no longer in use. Due to the lifecycle and MFA status of these enterprise applications, we were unable to verify the number that should be required to use MFA enforcement. The lack of MFA enforcement increases the risk of unauthorized access to information systems.

<u>RECOMMENDATIONS</u>

We recommend the Vice President, Chief Information and Digital Officer, IT:

1. Revise TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*, to include the appropriate reauthentication frequency and authorized exclusions.

2. Revise MFA enforcement access policies to include all networks as required by TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*.

3. Reconcile enterprise applications in Microsoft Entra® to validate their lifecycle and MFA status.

4. Implement a process to periodically validate the lifecycle and MFA status of enterprise applications in Microsoft Entra® with appropriate system owners and cloud administrators.

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.

- - - - - -

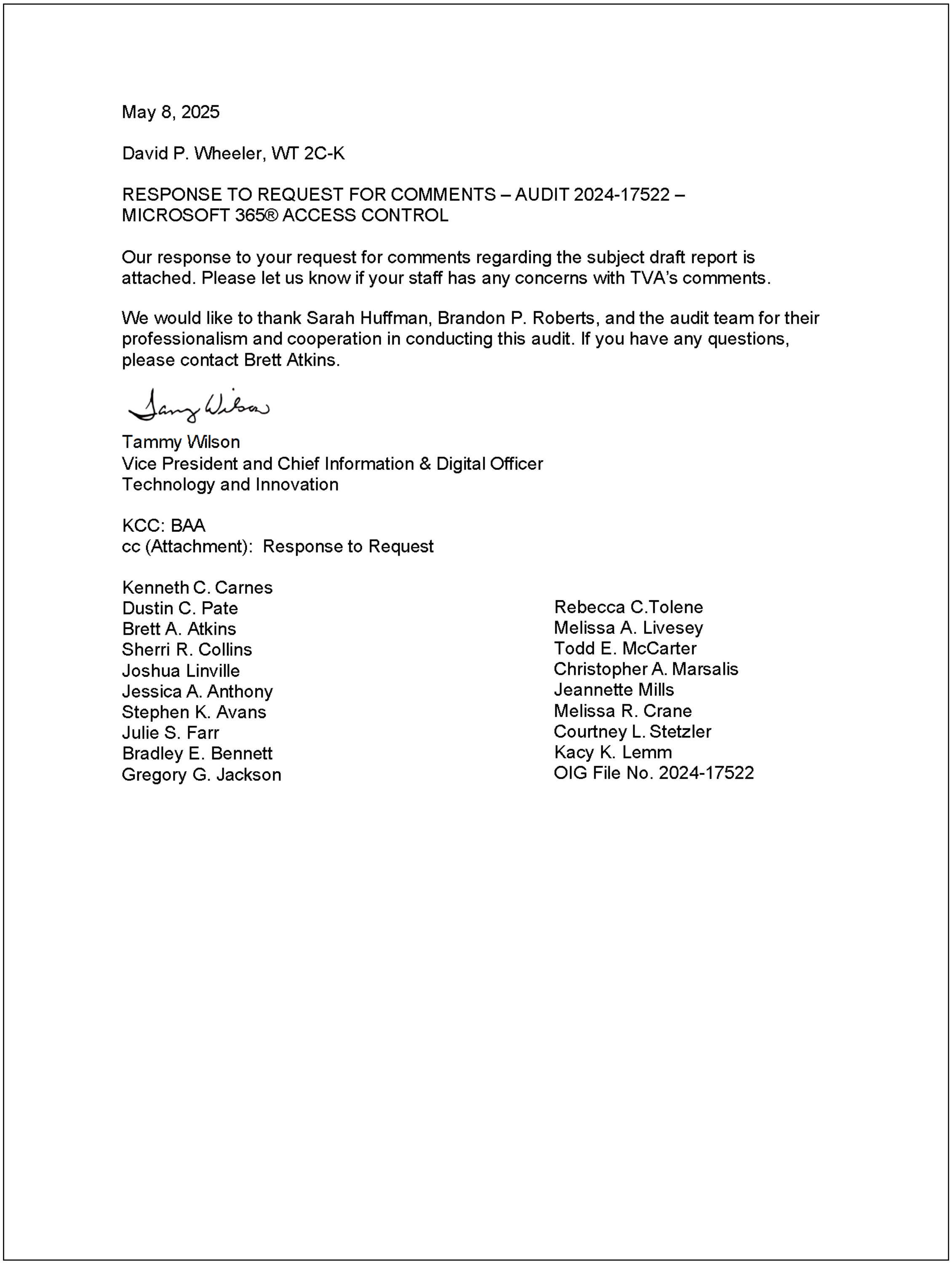
This report is for your review and information. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions, 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
cc: TVA Board of Directors
Brett A. Atkins
Kenneth C. Carnes
Sherri R. Collins
Melissa R. Crane
Jessica Dufner
Melissa A. Livesey
Jill M. Matthews
Todd E. McCarter
Jeannette Mills
Donald A. Moul
Dustin C. Pate
Ronald R. Sanders II
Courtney L. Stetzler
Josh Thomas
Rebecca C. Tolene
Ben R. Wagner
OIG File No. 2024-17522



May 8, 2025

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2024-17522 –
MICROSOFT 365® ACCESS CONTROL

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, Brandon P. Roberts, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.

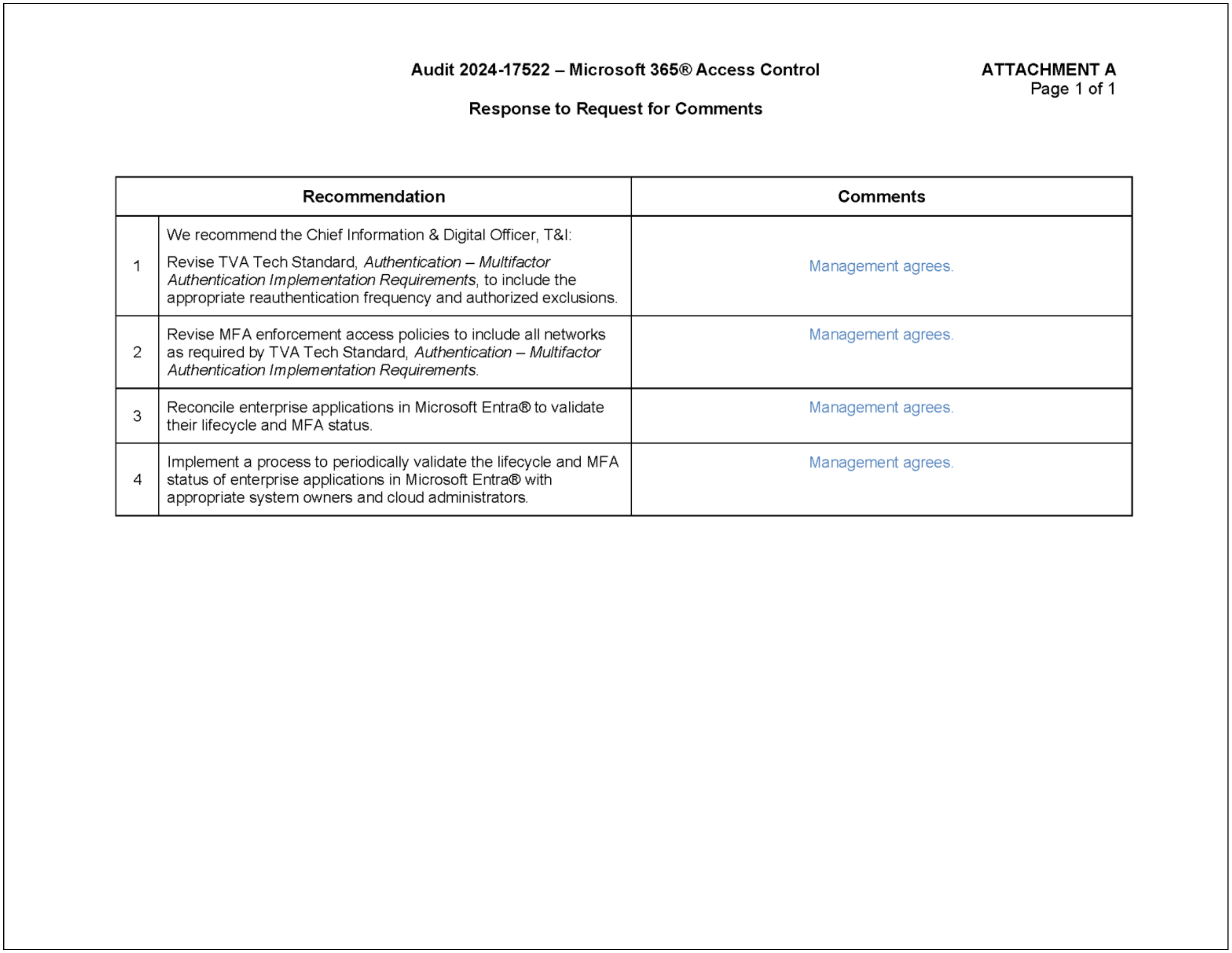
Tammy Wilson

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
Joshua Linville
Jessica A. Anthony
Stephen K. Avans
Julie S. Farr
Bradley E. Bennett
Gregory G. Jackson

Rebecca C.Tolene
Melissa A. Livesey
Todd E. McCarter
Christopher A. Marsalis
Jeannette Mills
Melissa R. Crane
Courtney L. Stetzler
Kacy K. Lemm
OIG File No. 2024-17522



Audit 2024-17522 – Microsoft 365® Access Control

ATTACHMENT A
Page 1 of 1

Response to Request for Comments

Recommendation		Comments
1	We recommend the Chief Information & Digital Officer, T&I: Revise TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*, to include the appropriate reauthentication frequency and authorized exclusions.	Management agrees.
2	Revise MFA enforcement access policies to include all networks as required by TVA Tech Standard, *Authentication – Multifactor Authentication Implementation Requirements*.	Management agrees.
3	Reconcile enterprise applications in Microsoft Entra® to validate their lifecycle and MFA status.	Management agrees.
4	Implement a process to periodically validate the lifecycle and MFA status of enterprise applications in Microsoft Entra® with appropriate system owners and cloud administrators.	Management agrees.