Memorandum from the Office of the Inspector General

June 21, 2023

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2022-17390 – REMOTE APPLICATION AND DESKTOP VIRTUALIZATION CLIENT

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority's (TVA) use of remote application and desktop virtualization client due to the risks of (1) potential system intrusion through misconfigurations and (2) continued elevated remote users during the COVID-19 pandemic. Our objective was to determine the effectiveness of TVA's remote application and desktop virtualization end user application security controls. The scope of this audit was limited to the management of remote end user components and applications, specifically the allowed access and security considerations in client configurations. Configuration management increases the security of individual computers, protects them from threats, and reduces the likelihood that a system will be compromised or that data will be disclosed to unauthorized parties. Fieldwork was performed from September 2022 through April 2023.

In summary, we found the configuration management control for TVA's remote application desktop virtualization client was ineffective. However, we determined compensating access controls were in place to mitigate the risk to an overall acceptable level. We recommend the Vice President and Chief Information and Digital Officer, Technology and Information (T&I), design and implement a documented configuration management process of TVA's remote application and desktop virtualization client. Specifics of the identified issues were 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 March 14, 2023.

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

BACKGROUND

TVA utilizes remote application and desktop virtualization software to provide workforce mobility while employees and contractors are not physically in the office. Virtualized environments include risks that must be mitigated at the architectural, configuration, and administrative levels to ensure secure access and minimize TVA's potential exposure from malicious activity, such as loss of sensitive or confidential information, damage to public image, or inappropriate access to critical TVA internal systems.

The management of remote end user components and applications, specifically the allowed access and security considerations in client configurations, can mitigate this risk. Configuration management increases the security of individual computers, protects them from threats, and reduces the likelihood that a system will be compromised or that data will be disclosed to unauthorized parties.

As part of our annual audit planning, we completed a threat assessment to identify high-risk cybersecurity threats that could potentially impact TVA. The potential for system intrusion through misconfigurations and changing workforce management were identified as higher risks in the threat assessment. Additionally, in 2021 we performed an audit to determine if TVA was following best practices to properly secure TVA's use of remote application and desktop virtualization.[1] We found several areas where TVA was consistent with cybersecurity remote access best practices. However, we identified gaps in TVA's configuration settings, architectural design, and administrative procedures. We made recommendations to T&I to review the identified gaps and remediate as appropriate.

The threat of system intrusion through misconfigurations combined with the continued elevated remote access use for TVA employees and contractors due to the COVID-19 pandemic caused an increased cybersecurity risk. Therefore, we included an audit of TVA's use of remote application and desktop virtualization client.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of TVA's remote application and desktop virtualization end user application security controls. The scope of this audit was limited to the management of remote end user components and applications, specifically the allowed access and security considerations in client configurations. Fieldwork was performed from August 2022 through April 2023. To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes to gain an understanding of TVA's processes related to remote access and account management.
- Inquired with TVA T&I personnel to gain an understanding of TVA's use of remote application and desktop virtualization, including walkthroughs of client configuration settings.
- Obtained current configuration settings of TVA's remote application and desktop virtualization client.
- Identified applicable vendor-provided remote access best practices and compared them to current configuration settings of TVA's remote application and desktop virtualization client software addressing security controls.

Configuration management was identified as an information system control that was significant to our audit objective. As such, it was included in our audit plan for 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

[1] Audit Report 2021-15804, *Remote Application and Desktop Virtualization,* January 11, 2022.

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 found the configuration management control for TVA's remote application desktop virtualization client was ineffective. Specifically, there were no documented processes for end user configuration reviews or updates. Additionally, TVA's end user baseline configurations were not aligned with applicable vendor-provided best practices. However, we determined compensating access controls were in place to mitigate the risk to an overall acceptable level.

The lack of a documented configuration management process could increase potential for fraud, intellectual property or personally identifiable information theft, cyber exploit, data loss, espionage, technological sabotage, and business disruption. Specifics of the identified issues were omitted from this report due to its sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on March 14, 2023.

RECOMMENDATION

We recommend the Vice President and Chief Information and Digital Officer, T&I, design and implement a documented configuration management process of TVA's remote application and desktop virtualization client.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendation. 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 Megan E. Spitzer, Senior Auditor, at (865) 633-7394 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the review.

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

MES:KDS
cc: See page 4

cc: TVA Board of Directors
Brett A. Atkins
Brandy A. Barbee
Faisal Bhatti
Andrea S. Brackett
Sherri R. Collins
Buddy Eller
David B. Fountain
Joshua Linville
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
John M. Thomas III
Josh Thomas
Ben R. Wagner
OIG File No. 2022-17390

June 14, 2023

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – Audit 2022-17390 – Remote Application and Desktop Virtualization Client

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

Jeremy Fisher
Vice President and Chief Information Officer
Technology and Innovation
SP 3A-C

ASB:BAA
cc (Attachment): Response to Request

Andrea Brackett, WT 5D-K
Faisal Bhatti
Brett A. Atkins
David B. Fountain
Gregory Jackson
Joshua Linville
Tangela Beasley
Brent Grim
Chetan Patel
Todd McCarter, MP 2C-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2022-17390

Audit 2022-17390
Remote Application and Desktop Virtualization
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: Design and implement a documented configuration management process of TVA's remote application and desktop virtualization client.	Management Agrees.