Memorandum from the Office of the Inspector General

January 11, 2022

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2021-15804 – REMOTE APPLICATION AND DESKTOP VIRTUALIZATION

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 due to the risk of increased remote users during the COVID-19 pandemic and recent publicized remote access vulnerabilities. Our objective was to determine if TVA was following best practices to properly secure TVA's use of remote application and desktop virtualization. Fieldwork was performed from May 2021 through November 2021.

In summary, 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 recommend the Vice President and Chief Information and Digital Officer, Technology and Information (T&I), review the identified gaps and remediate as appropriate. 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 November 15, 2021.

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.

Due the COVID-19 pandemic, there was an increase in remote access use for TVA employees and contractors. Additionally, there were recent publicized remote access vulnerabilities that could impact TVA. This combination causes an increased risk of potential exposure from malicious activity. Therefore, 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.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA was following best practices to properly secure TVA's use of remote application and desktop virtualization. The scope of this audit was limited to the management of remote application and desktop virtualization and did not include remote end user components and applications. Fieldwork was performed from May 2021 through November 2021. To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes (SPP) 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 the architectural design.
- Obtained current configuration settings of TVA's remote application and desktop virtualization software.
- Identified applicable vendor-provided remote access best practices and performed a gap analysis of TVA's processes and current configuration settings of TVA's remote application and desktop virtualization software addressing remote application and desktop virtualization.

Baseline configurations and configuration management were identified as information system controls that were significant to our audit objective. As such, they were 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 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 identified several areas where TVA was consistent with cybersecurity remote access best practices; however, we identified three gaps. The subject areas of identified gaps included (1) TVA's configuration settings, (2) architectural design, and (3) administrative procedures. 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 November 15, 2021.

RECOMMENDATIONS

We recommend the Vice President and Chief Information and Digital Officer, T&I, review the identified gaps and remediate as appropriate.

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

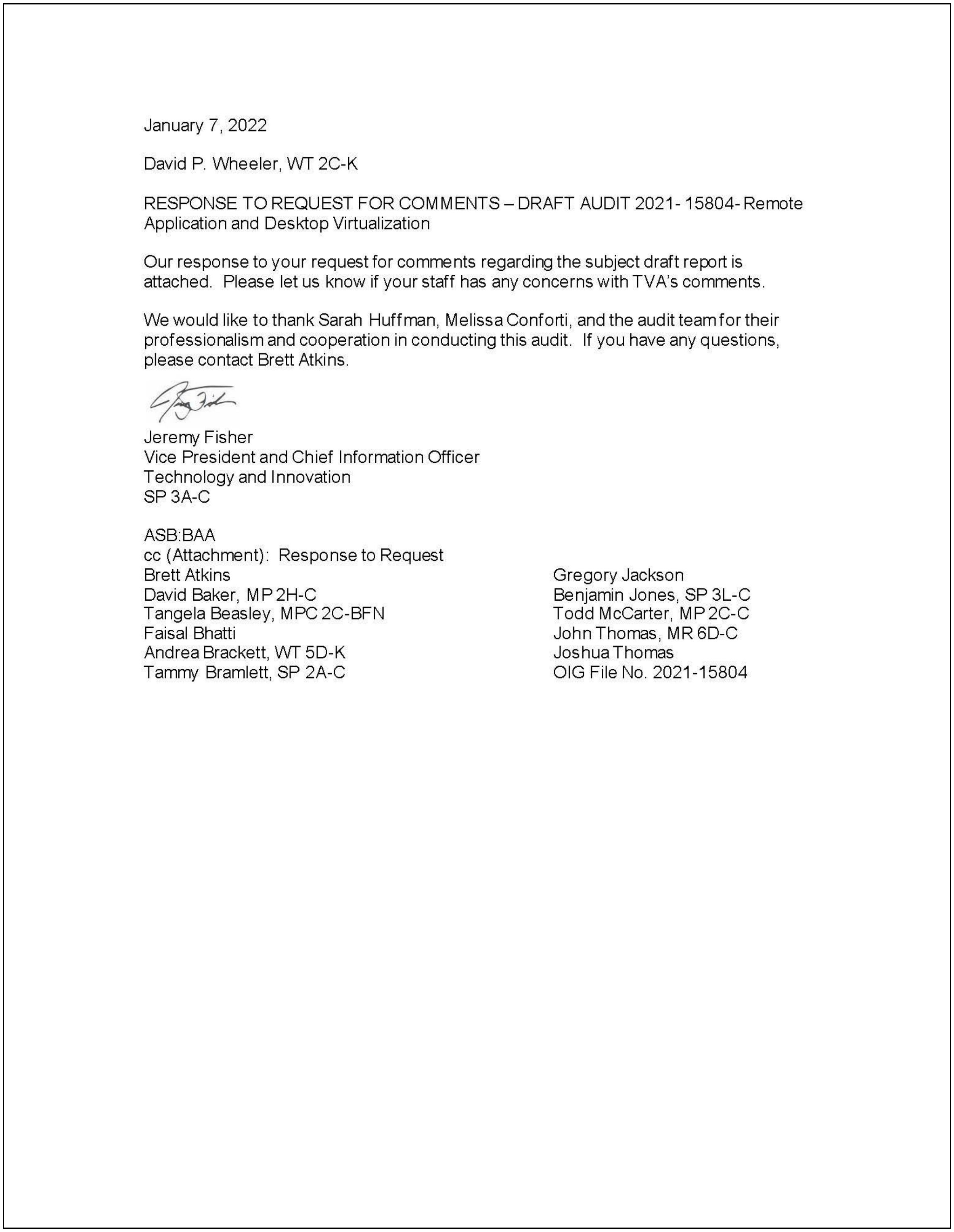
This report is for your review and information. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance. If you have any questions, please contact Melissa L. Conforti, Senior Auditor, at (865) 633-7383 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)

MLC:KDS
cc: TVA Board of Directors
Brett A. Atkins
David W. Baker
Brandy A. Barbee
Tangela Beasley
Faisal Bhatti
Andrea S. Brackett
Buddy Eller
David B. Fountain
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
John M. Thomas III
Josh Thomas
OIG File No. 2021-15804

APPENDIX
Page 1 of 2



January 7, 2022

David P. Wheeler, WT 2C-K

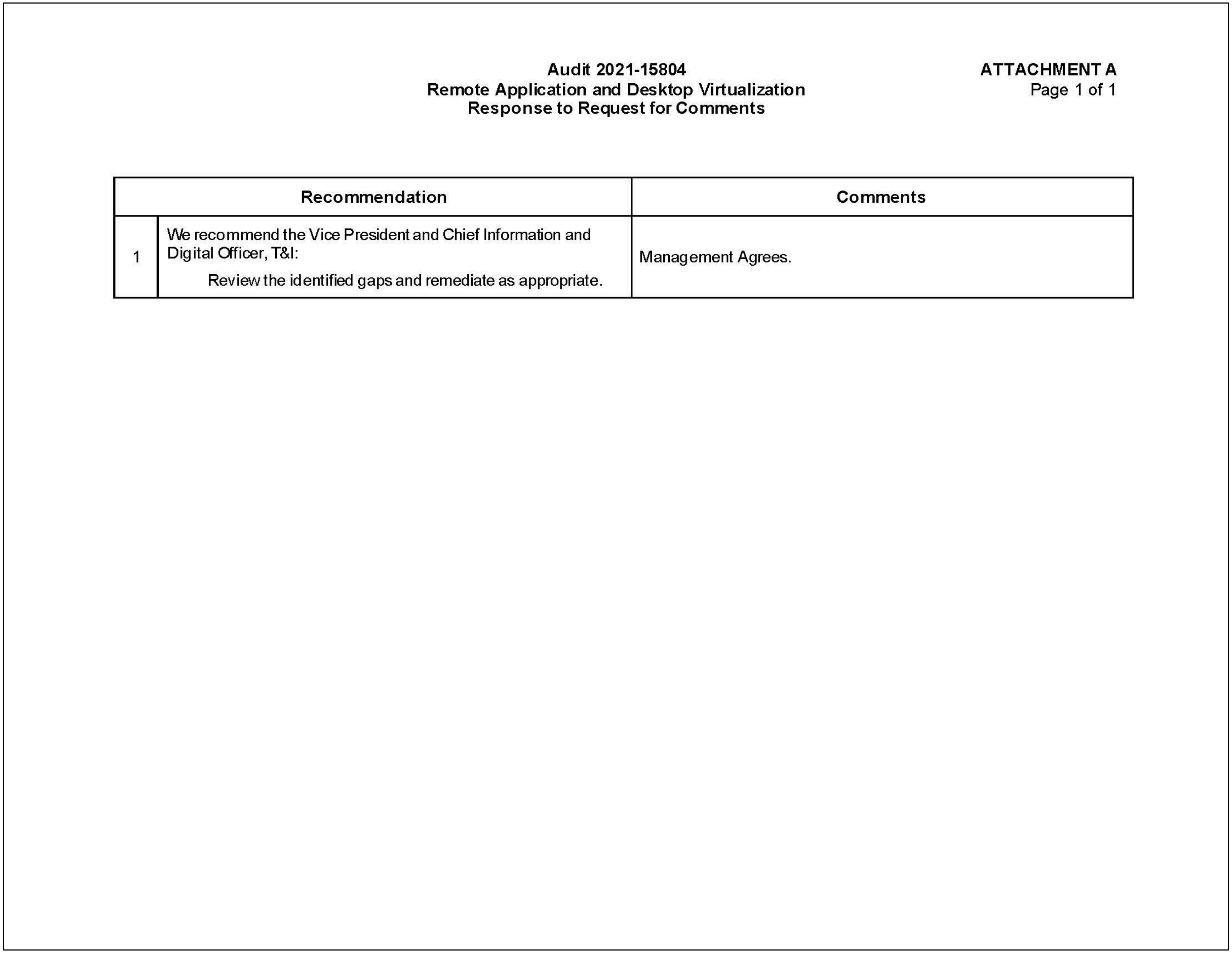
RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2021- 15804- Remote Application and Desktop Virtualization

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, Melissa Conforti, 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
Brett Atkins
David Baker, MP 2H-C
Tangela Beasley, MPC 2C-BFN
Faisal Bhatti
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Gregory Jackson
Benjamin Jones, SP 3L-C
Todd McCarter, MP 2C-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2021-15804



Audit 2021-15804
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: Review the identified gaps and remediate as appropriate.	Management Agrees.