Memorandum from the Office of the Inspector General

July 27, 2022

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2022-17338 – ENDPOINT PROTECTION

As part of our annual audit plan, we performed an audit of Tennessee Valley Authority's (TVA) endpoint protection. Our objective was to determine the effectiveness of endpoint protection on TVA desktops and laptops.

In summary, we found several areas of TVA's endpoint protection program to be generally effective, including the deployment of endpoint protection software, monitoring, and alerting. However, we identified two issues that should be addressed by TVA management to further increase the effectiveness of the endpoint protection program. We found (1) TVA does not require endpoint protection for all network connections and (2) gaps in TVA policy, procedures, and internal controls. 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 May 5, 2022. We recommend the Vice President and Chief Information and Digital Officer, Technology and Innovation (T&I) (1) implement endpoint-protection requirements for all network connections on T&I managed desktops and laptops and (2) implement and/or update policy, procedure, and internal control documentation for endpoint protection.

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

BACKGROUND

According to the National Institute of Standards and Technology (NIST), endpoints (e.g., laptops, desktops) are a fundamental part of any organizational information technology system. Endpoints are an important source of connecting end users to networks and systems, are a major source of vulnerabilities, and a frequent target of attackers looking to penetrate a network. User behavior is difficult to control and hard to predict. User actions, whether clicking a link that executes malware or changing a security setting to improve the usability of the endpoint, frequently allow exploitation of vulnerabilities.[1]

As part of our annual audit planning, we completed a threat assessment to identify cybersecurity risks and threats that could potentially impact TVA. Our threat assessment also included results from TVA's enterprise risk-management process. The potential for

[1] NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011

system intrusion through vulnerable workstations was one of the risk areas identified. Therefore, we included an audit of TVA's endpoint protection of desktops and laptops as part of our 2022 audit plan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of endpoint protection on TVA desktops and laptops. The scope of our audit was the endpoint protection software on T&I managed desktops and laptops and the applications used to manage endpoint protection software. Fieldwork was completed between January 2022 and April 2022. To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes and internal control documentation to gain an understanding of TVA's processes related to endpoint protection.
- Inquired with TVA T&I personnel to gain an understanding of TVA's use of endpoint protection systems.
- Performed system walkthroughs to identify and obtain information on endpoint protection processes.

During audit planning, we identified one information technology control area (endpoint protection) significant to the objectives of our audit and performed testing to determine control effectiveness.

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 found several areas of TVA's endpoint protection program to be generally effective including the deployment of endpoint protection software, monitoring, and alerting. However, we identified two issues that should be addressed by TVA management to further increase the effectiveness of the endpoint protection program. 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 May 5, 2022.

TVA DOES NOT REQUIRE ENDPOINT PROTECTION FOR ALL NETWORK CONNECTIONS

We found TVA had deployed endpoint protection software on desktops and laptops; however, it is not enforced on all types of network connections. Office of Management and Budget's memorandum 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, highlights the importance of endpoint detection and response, and requires that endpoint detection and response tools "are deployed and operated across their enterprise." TVA uses a product to ensure that endpoints have endpoint protection software on some network connections, but does not have technical requirements to enforce these requirements on all network connections. This could allow unprotected desktops and laptops to connect to the network increasing the risk of propagating malware on TVA networks.

GAPS IDENTIFIED IN ENDPOINT PROTECTION POLICY, PROCEDURES, AND INTERNAL CONTROL

We found TVA previously had policy requirements for endpoint protection. However, during a recent policy update, endpoint protection requirements were removed, and TVA does not currently have policy requirements for endpoint protection. NIST[2] requires policies and procedures for system and information integrity that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. In addition, TVA's internal control documentation has not been updated to align with TVA's technical implementation of endpoint protection. Policies and procedures bring uniformity to operations and reduce the risk of an unwanted event (e.g., computer virus or malware).

RECOMMENDATIONS

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

1. Implement endpoint protection requirements for all network connections on T&I managed desktops and laptops.

2. Implement and/or update policy, procedure, and internal control documentation for endpoint protection.

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.

- - - - - -

[2] NIST Special Publication 800-53 (Revision 5), *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020.

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.

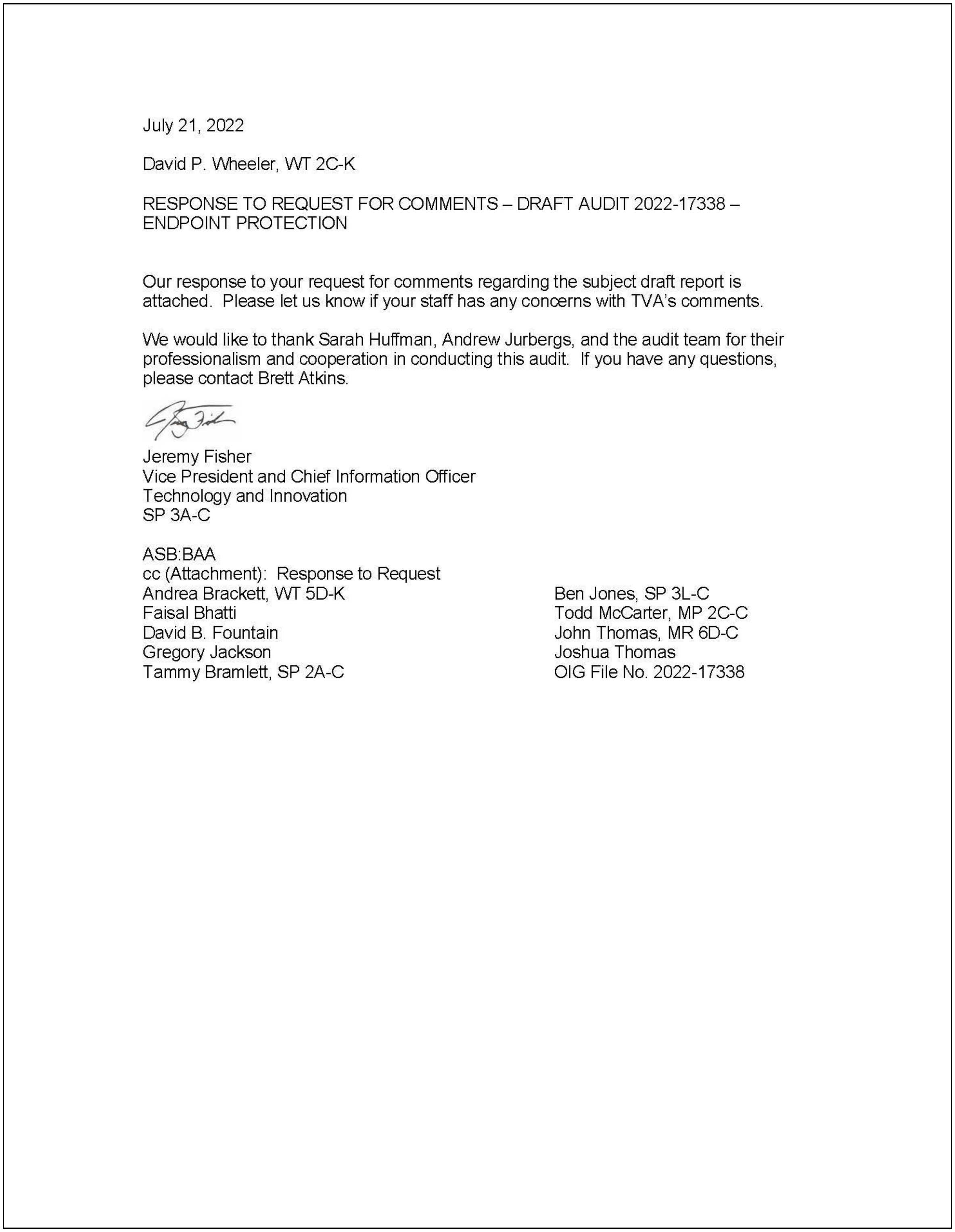
If you have any questions or need additional information, please contact Andrew J. Jurbergs, Senior Auditor, at (865) 633-7393 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler

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

AJJ:KDS
cc: TVA Board of Directors
Brett A. Atkins
Brandy A. Barbee
Faisal Bhatti
Andrea S. Brackett
Sherri R. Collins
Buddy Eller
David B. Fountain
Jim R. Hopson
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
John M. Thomas III
Josh Thomas
Ben R. Wagner
OIG File No. 2022-17338

APPENDIX
Page 1 of 1



July 21, 2022

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2022-17338 – ENDPOINT PROTECTION

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, Andrew Jurbergs, 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
David B. Fountain
Gregory Jackson
Tammy Bramlett, SP 2A-C
Ben Jones, SP 3L-C
Todd McCarter, MP 2C-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2022-17338

APPENDIX
Page 1 of 1

ATTACHMENT A
Page 1 of 1

Audit 2022-17338
ENDPOINT PROTECTION
Response to Request for Comments

Recommendation		Comments
1	We recommend the Vice President and Chief Information and Digital Officer, T&I: Implement endpoint protection requirements for all network connections on T&I managed desktops and laptops.	Management agrees.
2	We recommend the Vice President and Chief Information and Digital Officer, T&I: Implement and/or update policy, procedure, and internal control documentation for endpoint protection.	Management agrees.