Memorandum from the Office of the Inspector General

September 24, 2021

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2021-15778 – WINDOWS®
DESKTOP AND LAPTOP PATCHING

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority's (TVA) patching of Windows® desktops and laptops. Our objective was to determine if high-risk vulnerabilities on desktops and laptops were patched in accordance with TVA policy and best practices. Patching is the process for updating products and systems. Patches correct security and functionality problems in software and firmware. We reviewed TVA's policies and procedures against best practices, reviewed TVA's inventory of Windows® desktops and laptops, and performed analysis of TVA's patching performance over the period of March 2020 through March 2021.

In summary, we found (1) TVA policies and procedures aligned with best practices, (2) the majority of Windows® desktops and laptops managed by TVA's automated patching system were patched for high-risk vulnerabilities in accordance with TVA policy, and (3) TVA had mitigated vulnerabilities for Windows® desktops and laptops that had not received updates. However, although the majority of Windows® workstations were managed by TVA's automated patching system, we found some desktops and laptops were at potential risk of compromise. The 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 briefings on July 13, 2021, and July 20, 2021.

We recommend the Vice President and Chief Information and Digital Officer, Technology and Innovation (T&I), update processes to identify and address Windows® devices that are not managed by TVA's automated patching system.

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

BACKGROUND

The National Institute of Science and Technology (NIST) states that, "patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they mitigate software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation."[1]

Patching has been an area of concern in previous audits. In our 2016 FISMA audit,[2] we were unable to test the patch management process because it had not been fully implemented. In our 2016 audit[3] on cyber security patch management of high-risk desktops and laptops, we found TVA desktops and laptops were not being managed by TVA's patch management tools.

According to the T&I system of record for inventory, TVA has over 10,000 Windows® desktops and laptops in use. TVA procedure requires T&I to utilize automated solutions to maintain application management/inventory and scan the desktop environment to determine the version/patch level of the operating system and applications. The Information Technology Asset Administrator is responsible for keeping the system of record for inventory. Windows® desktops and laptops are updated through an automated patching system that identifies applicable updates and deploys them on a scheduled basis.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if high-risk vulnerabilities on Windows® desktops and laptops were patched in accordance with TVA policy and best practices. The scope of this audit was limited to desktops and laptops running Windows® that are managed by TVA's T&I organization. Fieldwork was performed between December 2020 and July 2021.

To achieve our objective, we:

- Obtained and reviewed TVA Standard Programs and Processes (SPP), T&I policies, procedures, and work instructions (WI) including:
  - TVA-SPP-12.001, A*cceptable Use of Information Resources.*
  - TVA-SPP-12.004, *TVA Cybersecurity Patch and Vulnerability Management Program.*
  - Information Technology (IT) WI-12.342, *Windows® Desktop Patch Management.*
- Performed a gap analysis comparing T&I policies and technical procedures against best practices.[4]

[1] Murugiah Souppaya and Karen Scarfone, "Guide to Enterprise Patch Management Technologies," *NIST Special Publication 800-40,* Revision 3, July 2013, page iii, <http://dx.doi.org/10.6028/NIST.SP.800-40r3>, accessed on January 20, 2021.

[2] Audit Report 2016-15407, *Federal Information Security Management Act*, January 11, 2017

[3] Audit Report 2016-15369, *Cyber Security Patch Management of High-Risk Desktops and Laptops*, July 19, 2017.

[4] Best practices used in the audit included guidelines released by the National Institute of Standards and Technology (NIST),Cybersecurity Framework, an organization that develops and maintains an extensive collection of standards, guidelines, recommendations, and research on the security and privacy of information and information systems.

- Interviewed IT personnel and performed process walkthroughs to identify and obtain information on TVA's controls for updating Windows® desktops and laptops.
- Identified and tested controls in place related to inventory and patch management.
- Reviewed data from the system of record for inventory and reconciled it against TVA's system for controlling access to network resources and the automated patch management system.
- Compared Windows® high-risk updates deployed by TVA against the Microsoft® critical and important patch release dates for the Windows® operating system.
- Reviewed TVA's policies for patch management and compared them against TVA's practices to determine if policy was followed.
- Reviewed TVA's vulnerability scanning system results to identify patch mitigation records and active vulnerabilities.

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 (1) TVA policies and procedures aligned with best practices, (2) the majority of Windows® desktops and laptops managed by TVA's automated patching system were patched for high-risk vulnerabilities in accordance with TVA policy during the period of March 2020 through March 2021, and (3) TVA had mitigated vulnerabilities for Windows® desktops and laptops that had not received updates. However, although the majority of Windows® workstations were managed by TVA's automated patching system, we found some desktops and laptops were at potential risk of compromise.

TVA AT POTENTIAL RISK OF COMPROMISE DUE TO WINDOWS® DESKTOPS AND LAPTOPS NOT BEING IN PATCH MANAGEMENT SYSTEM

We reconciled the inventory of Windows® desktops and laptops from T&I's automated patch management system and Windows® Active Directory and determined the majority of Windows® desktops and laptops were managed by TVA's automated patching system. However, we found not all Windows® laptops and desktops were being managed by the automated patching system. IT-WI-12.342, *Windows® Desktop Patch Management*, requires T&I to utilize automated solutions to maintain application management/inventory and scan the desktop environment to determine the version/patch level of the operating system and applications.

Further, TVA-SPP-12.004, *TVA Cybersecurity Patch and Vulnerability Management Program*, requires vulnerability management to reduce or eliminate cyber vulnerabilities through patching or implementation of other remediation recommendations. In addition, NIST SP 800-40 rev. 3 states that if an attacker discovers the same vulnerability before the patch is released, the attacker may have a longer window of opportunity to exploit the vulnerability because of the intentional delay in releasing the patch.

Prior to the completion of our audit, TVA management identified a failure in a process intended to correct and reconcile inventory discrepancies and took action to resolve this failure. We confirmed this action would remediate some, but not all, of the exceptions we found.

The specifics of the findings and testing performed have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in briefings on July 13, 2021, and July 20, 2021.

RECOMMENDATION

We recommend the Vice President and Chief Information and Digital Officer, T&I, update processes to identify and address Windows® devices that are not managed by TVA's automated patching system.

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.

- - - - - -

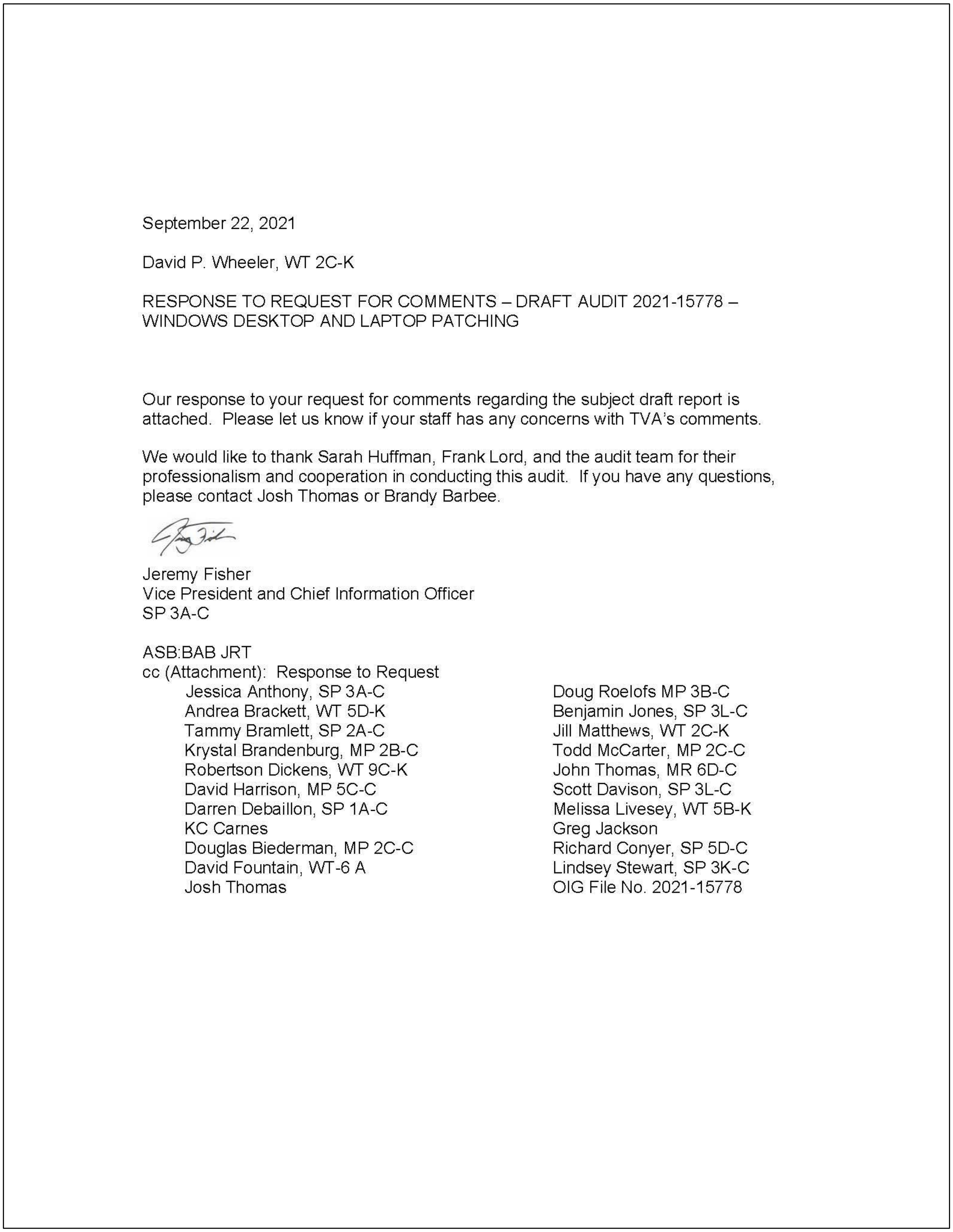
This report is for your review and information. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance. If you have any questions, please contact Frank B. Lord, Auditor, at (865) 633-7397 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.

Curtis C Hudson

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

FBL:KDS
cc: TVA Board of Directors
Andrea S. Brackett
Melissa R. Crane
Buddy Eller
David B. Fountain
Greg G. Jackson
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Douglas E. Roelofs
Lindsey M. Stewart
John M. Thomas III
OIG File No. 2021-15778

APPENDIX
Page 1 of 2



September 22, 2021

David P. Wheeler, WT 2C-K

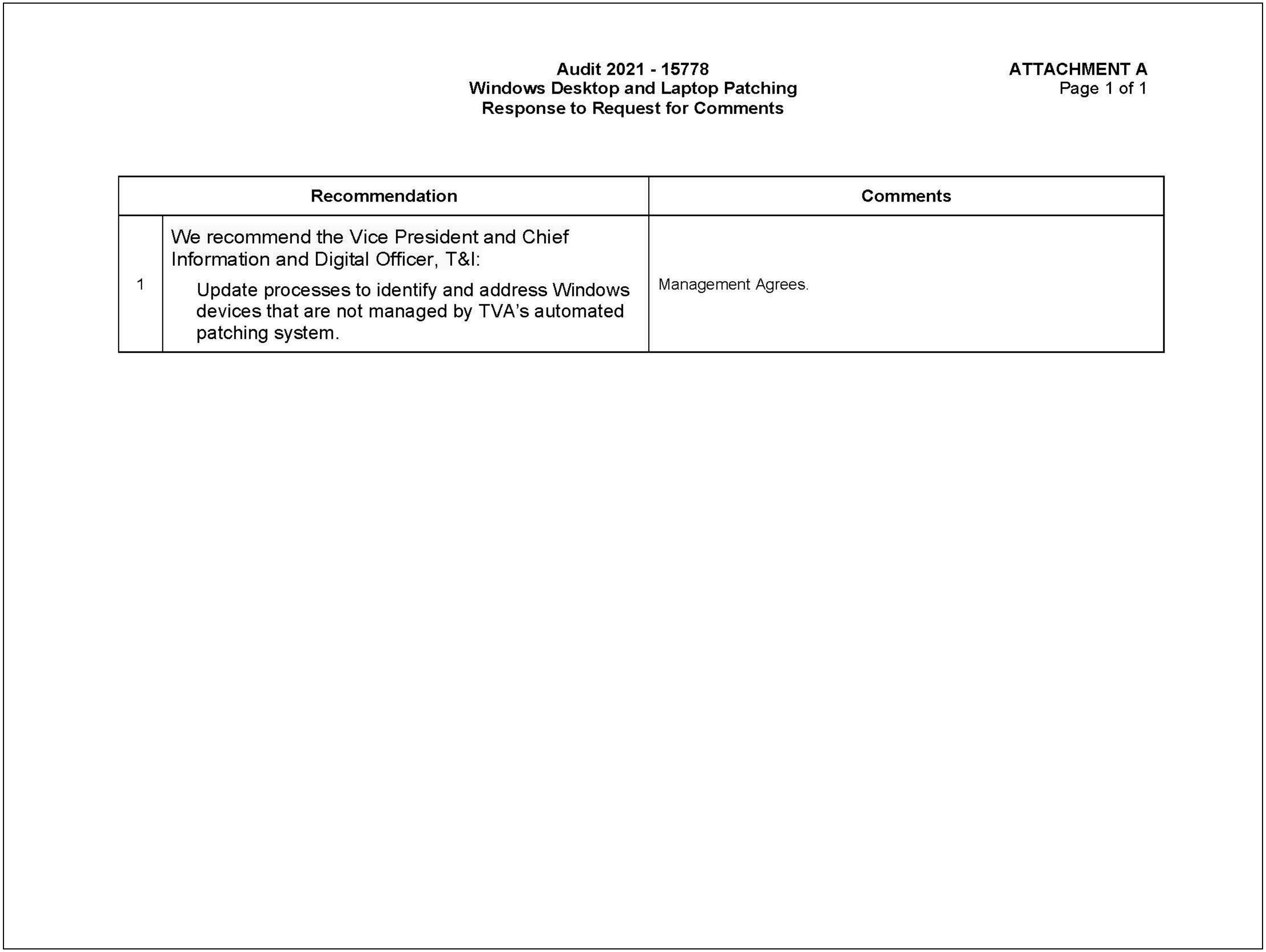
RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2021-15778 – WINDOWS DESKTOP AND LAPTOP PATCHING

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, Frank Lord, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Josh Thomas or Brandy Barbee.

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

ASB:BAB JRT
cc (Attachment): Response to Request
Jessica Anthony, SP 3A-C
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C
Darren Debaillon, SP 1A-C
KC Carnes
Douglas Biederman, MP 2C-C
David Fountain, WT-6 A
Josh Thomas
Doug Roelofs MP 3B-C
Benjamin Jones, SP 3L-C
Jill Matthews, WT 2C-K
Todd McCarter, MP 2C-C
John Thomas, MR 6D-C
Scott Davison, SP 3L-C
Melissa Livesey, WT 5B-K
Greg Jackson
Richard Conyer, SP 5D-C
Lindsey Stewart, SP 3K-C
OIG File No. 2021-15778



Audit 2021 - 15778
Windows Desktop and Laptop Patching
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: Update processes to identify and address Windows devices that are not managed by TVA's automated patching system.	Management Agrees.