



Memorandum from the Office of the Inspector General

January 30, 2025

Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2024-17508 – CYBERSECURITY VULNERABILITY MANAGEMENT

Due to potential cybersecurity risks, we performed an audit of the Tennessee Valley Authority's (TVA) cybersecurity vulnerability management program. Our objective was to determine if TVA is compliant with the Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*¹ (KEVs), and CISA BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*.² Our scope for this audit was limited to the compliance and cybersecurity activities related to CISA BOD 19-02 and CISA BOD 22-01 performed within TVA's Technology and Innovation (T&I) organization.

We determined TVA generally complied with CISA BOD 19-02 and CISA BOD 22-01; however, two requirements were not fully met. Specifically, TVA did not (1) update CISA with modifications to the inventory of internet-accessible internet protocol³ (IP) addresses within the five-day requirement or (2) meet the CISA required remediation timeline for 8 of 22 KEVs. We recommend the Vice President and Chief Information and Digital Officer, T&I, (1) design and implement a documented process for maintaining an accurate inventory of internet-accessible IP addresses and update CISA within five days of changes and (2) update patch management processes to verify KEVs are patched or mitigated in accordance with policy.

TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

BACKGROUND

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. CISA is designed for collaboration and partnership and has a layered mission to reduce risk to the nation's cyber and physical infrastructure. As a federal agency in the civilian Executive Branch, TVA is required to comply with CISA BODs.

¹ CISA BOD 22-01 *Reducing the Significant Risk of Known Exploited Vulnerabilities*, November 3, 2021, <<https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities>>, accessed on June 25, 2024.

² CISA BOD 19-02 *Vulnerability Remediation Requirements for Internet-Accessible Systems*, April 29, 2019, <<https://www.cisa.gov/news-events/directives/bod-19-02-vulnerability-remediation-requirements-internet-accessible-systems>>, accessed on June 25, 2024.

³ An IP address represents a computer's location on the Internet.

CISA BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, requires federal agencies to ensure CISA is given access to scan an accurate listing of the agency's internet-accessible IP addresses to identify vulnerabilities. Any modifications to the listing must be reported to CISA within five days. Agencies must remediate CISA identified critical or high vulnerabilities within 15 or 30 days of detection, respectively.

CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, requires federal agencies to remediate vulnerabilities from the CISA-managed KEV catalog in accordance with remediation timelines. According to CISA BOD 22-01, KEVs "carry significant risk to the federal enterprise," and CISA determines "vulnerabilities warranting inclusion in the catalog based on reliable evidence that the exploit is being actively used to exploit public or private organizations by a threat actor."

Due to potential cybersecurity risks, we performed an audit of TVA's cybersecurity vulnerability management program.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA was compliant with CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, and CISA BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*. Our scope for this audit was limited to the compliance and cybersecurity activities related to CISA BOD 19-02 and CISA BOD 22-01 performed within TVA's T&I organization. To achieve our objective, we:

- Reviewed the following TVA Standard Programs and Processes (SPPs) to gain an understanding of TVA's requirements related to vulnerability management:
 - TVA-SPP-12.004, *TVA Cybersecurity Vulnerability Management Program*
 - TVA-SPP-12.806, *TVA Cybersecurity Patch and Remediation Management Program*
- Performed a gap analysis between CISA BODs and TVA SPPs to determine if TVA policy included the BOD requirements.
- Inquired of TVA T&I personnel to gain an understanding of TVA's vulnerability management program. Specifically for understanding the processes around:
 - Developing and maintaining TVA's list of public facing IP addresses.
 - Tracking and remediating KEVs.
- Reviewed TVA vulnerability scan data related to KEVs.
- Identified internal control to be significant to the audit and performed testing to the extent necessary to address the audit objective, including:
 - Identified vulnerability assessment and remediation as key information systems controls.
 - Assessed design of internal controls by reviewing TVA policy to determine if the controls, as designed, were meeting their intended objectives.

- Assessed implementation and operating effectiveness of internal controls to determine if the required actions in the BODs were being performed.
- Assessed TVA's compliance with the agency requirements in CISA BOD 19-02 and CISA BOD 22-01.

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 determined TVA generally complied with CISA BOD 19-02 and CISA BOD 22-01; however, two requirements were not fully met. Specifically, TVA did not (1) update CISA with modifications to the inventory of internet-accessible IP addresses within the five-day requirement or (2) meet the CISA required remediation timeline for 8 of 22 KEVs due during the audit.

TVA DID NOT UPDATE CISA IN ACCORDANCE WITH CISA BOD 19-02

CISA BOD 19-02 requires federal agencies to remove CISA vulnerability scanner source IP addresses from block lists to ensure CISA access, notify CISA of any modifications to internet-accessible IP addresses, and remediate public-facing vulnerabilities. While TVA has given access to CISA to perform vulnerability scans against internet-accessible IP addresses, TVA did not have a documented process for developing and maintaining its internet-accessible systems inventory and did not include cloud hosted systems. As a result, TVA did not update CISA about modifications to the agency's inventory of internet-accessible IP addresses within the five-day BOD 19-02 requirement. An inaccurate inventory of public-facing IP addresses could result in unauthorized access by exploiting unidentified vulnerabilities in systems not scanned by CISA.

During the audit, there were no critical or high public-facing vulnerabilities for TVA to remediate. Therefore, we were unable to assess compliance with this part of CISA BOD 19-02.

TVA DID NOT MEET REMEDIATION TIMELINES IN ACCORDANCE WITH CISA BOD 22-01

CISA BOD 22-01 requires federal agencies to review and update vulnerability management procedures, assign roles/responsibilities for agency actions, track and report to CISA as needed, and remediate KEVs within defined timelines. TVA has (1) designed policies, including roles and responsibilities in compliance with the BOD and (2) automated KEV reporting to CISA. However, we determined the internal control for vulnerability remediation needed improvement. Specifically, we reviewed TVA vulnerability scan data and found 8 of 22 KEVs had not been fully remediated in accordance with CISA timelines because TVA did not verify KEVs were patched or mitigated in a timely manner. As of the date we reviewed the vulnerability scan data,

these KEVs accounted for 979 instances of vulnerabilities on the TVA network that could potentially be used to exploit systems.

RECOMMENDATIONS

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

1. Design and implement a documented process for maintaining an accurate inventory of internet-accessible IP addresses and update CISA within five days of changes.
2. Update patch management processes to verify KEVs are patched or mitigated in accordance with policy.⁴

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 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
Assistant Inspector General
(Audits and Evaluations)

AJJ:KDS

cc: TVA Board of Directors
Brett A. Atkins
Faisal Bhatti
Kenneth C. Carnes II
Sherri R. Collins
Buddy Eller
David B. Fountain
Melissa L. Livesey

Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Jeannette Mills
Dustin C. Pate
Josh Thomas
Ben R. Wagner
OIG File No. 2024-17508

⁴ Prior to receiving TVA's response to our draft audit report, we had discussions with TVA management regarding clarification of Recommendation No. 2 and revised the recommendation accordingly.

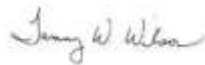
January 23, 2025

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2024-17508 –
CYBERSECURITY VULNERABILITY MANAGEMENT

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.



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
Faisal Bhatti
Bradley E. Bennett

David B. Fountain
Gregory G. Jackson
Melissa A. Livesey
Todd E. McCarter
Christopher A. Marsalis
Jeannette Mills
Melissa R. Crane
Courtney L. Stetzler
Kacy K Kirtley
OIG File No. 2024-17508

Audit 2024-17508 – Cybersecurity Vulnerability Management
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	We recommend the Vice President and Chief Information & Digital Officer, T&I: Design and implement a documented process for maintaining an accurate inventory of internet-accessible IP addresses and update CISA within five days of changes.	Management agrees.
2	Update the vulnerability management process to ensure KEVs are patched or mitigated in a timely manner.	Management agrees to update patch management processes to verify KEVs are patched or mitigated in accordance with policy.