Memorandum from the Office of the Inspector General

June 1, 2022

James R. Dalrymple
Jeremy P. Fisher

REQUEST FOR FINAL ACTION – AUDIT 2022-17340 – NON-POWER DAM CONTROL SYSTEM CYBERSECURITY

As part of our annual audit plan, we performed an audit of Tennessee Valley Authority's (TVA) non-power dam control system cybersecurity. Our objective was to determine if the cybersecurity controls of TVA's non-power dam control system were operating effectively.

In summary, we found (1) no clear ownership of the non-power dam control system, (2) vulnerable versions of operating systems and control system software, (3) inappropriate logical and physical access, and (4) internal information technology controls were not operating effectively or had not been designed and implemented. Prior to completion of our audit, TVA clarified the ownership of the control system and took actions to address the inappropriate logical and physical access. We recommend the Senior Vice President, Resource Management and Operations Services, update the non-power dam control system to address the identified vulnerabilities and information technology control weaknesses. 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 April 12, 2022.

In response to our draft report, TVA management agreed with the recommendation in the report and provided information on planned actions. See the Appendix for TVA management's complete response.

BACKGROUND

TVA's mission includes being a steward of the regions' natural resources, which includes managing the Tennessee River system to provide multiple benefits including flood control, recreation, and power production. To assist in the management of the river system, TVA operates a control system to manage the water flow from various dams that do not provide hydroelectric power.

As part of our annual audit planning, we completed a threat assessment to identify high-risk cybersecurity threats that could potentially impact TVA. Our threat assessment also included results from TVA's enterprise risk management process. The potential for the exploitation of TVA operated control systems was one of the high-risk areas identified. Therefore, we included an audit of TVA's non-power dam control system as part of our 2022 audit plan.

In discussions with TVA management, we identified various non-power dams operated by the control system under review. During those discussions we determined that risks related to river management would be low based on their location, size, and existing physical controls that limit water flow adjustments. However, unauthorized access events pose a high reputational risk for TVA.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if the cybersecurity controls of TVA's non-power dam control system were operating effectively. The scope of our audit was the non-power dams that are operated by an off-site control system. Fieldwork was completed between December 2021 and April 2022. To meet our objective we:

- Inquired of TVA personnel to gain an understanding of the control system and dams it controls.
- Reviewed documentation related to the control system to gain an understanding of how the control system operates.
- Reviewed logical access to the control system to determine appropriateness.
- Reviewed physical access to the control system to determine appropriateness.
- Reviewed vulnerability reports to identify risks.
- Observed control system operating systems and software to gain an understanding of how the control system operates and how it is configured.
- Observed physical access controls for appropriateness.

During audit planning, we identified four information technology control areas (access management, patch management, configuration management, and contingency planning) 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 (1) no clear ownership of the non-power dam control system, (2) vulnerable versions of operating systems and control system software, (3) inappropriate logical and physical access, and (4) information technology controls were not operating effectively or had not been designed and implemented. The specifics of the findings and testing performed have been omitted from this report due to their sensitive nature to TVA's cybersecurity, but were formally communicated to TVA management in a briefing on April 12, 2022.

CONTROL SYSTEM OWNERSHIP UNCLEAR

We found two different TVA teams were involved in the design, maintenance, and operation of the non-power dam control system, but there was no clear ownership of the system. Without clear ownership, the maintenance and operation of cybersecurity controls may not occur, increasing cybersecurity risks related to the control system. Prior to completion of our audit, TVA management took action to clarify non-power dam control system ownership.

VULNERABLE OPERATING SYSTEMS AND SOFTWARE

We found operating system and control system software vulnerabilities that could be used to gain inappropriate access to the non-power dam control system, allowing for adjustments to water flows that could potentially have a negative impact on river management. TVA reputational risk would be high if such an event was publicized.

INAPPROPRIATE LOGICAL AND PHYSICAL ACCESS

We found TVA personnel with inappropriate logical access to the non-power dam control system or inappropriate physical access to the control system's location. In addition, we found that a default TVA organization still had responsibility for approving and reviewing physical access to this location. Prior to completion of our audit, TVA management took action to (1) remove the inappropriate logical access and (2) assign the responsibility of approving and reviewing physical access to the appropriate team. In addition, TVA management informed us they will review physical access for appropriateness.

INFORMATION TECHNOLOGY CONTROL WEAKNESSES

Based on our testing of information technology controls, we found that contingency planning controls were appropriately designed, implemented, and operating effectively. However, we found that while controls for access management were appropriately designed and implemented, they were not operating effectively. In addition, we found that controls for patch management and configuration management had not been designed.

RECOMMENDATION

We recommend the Senior Vice President, Resource Management and Operations Services, update the non-power dam control system servers to address identified vulnerabilities and internal control weaknesses.

TVA Management's Comments – In response to our draft report, TVA management agreed with the recommendation in the report and provided information on planned actions. See the Appendix for TVA management's complete response.

- - - - - -

This report is for your review and final action. Your written comments, which addressed your management decision and actions planned or taken, have been included in the report. Please notify us when final action is complete. 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 wish to discuss our observations, please contact Scott A. Marler, Audit Manager, at (865) 633-7352 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)

SAM:KDS
cc: TVA Board of Directors
Brett A. Atkins
Brandy A. Barbee
Faisal Bhatti
Andrea S. Brackett
Catherine Butler
Allen A. Clare
Samuel P. Delk
Buddy Eller
James H. Everett
David B. Fountain
Prentice Gilbert
Kelie H. Hammond
Jeffery J. Lyash
Jill M. Matthews
Todd E. McCarter
Donald A. Moul
Preston P. Pratt
Ronald A. Sanders II
Jeffry W. Stichler
John M. Thomas III
Josh Thomas
Kay W. Whittenburg
Dennis H. Yankee
OIG File No. 2022-17340

May 25, 2022

David P. Wheeler, WT 2C-K

RESPONSE TO DRAFT EVALUATION 2022-17340 – NON-POWER DAM CONTROL SYSTEM CYBERSECURITY

Thank you for the opportunity to address the recommendation from the Draft Evaluation 2022-17340-Non-Power Dam Control System Cybersecurity. After reviewing the report, we agree with the recommendation and included the actions to be taken. We would like to thank Scott Marler and his team for their professionalism and cooperation during this audit.

GENERAL COMMENTS
Regarding the finding control system ownership unclear: Clear ownership, roles and responsibilities will be documented within existing system documentation.

RECOMMENDATION 1
We recommend the Senior Vice President, Resource Management and Operations Services, update the non-power dam control system servers to address identified vulnerabilities and internal control weaknesses.

Response Actions:

We agree with this recommendation and will take the following steps:

- Work with software vendor to update or replace the current software version to achieve compliance with latest cyber security standards. Due date May 27, 2023.
- Incorporate the SCADA System in the River Forecasting System Security Plan to provide alignment to cyber standards, and support from TVA T&I resources for patching and configuration control. Due date May 27, 2023.

This memorandum provides acceptance of the noted recommendation and actions to be taken. If you have further questions, please contact James R. (Bob) Dalrymple, Senior Vice President, Resource Management and Operations Services.

James R. Dalrymple
Senior Vice President
Resource Management and Operations Services
BR 4D-C

RRS:ALH

cc: Brett A. Atkins, MP 2C-C
Brandy A. Barbee, MP 2B-C
Faisal Bhatti, SP 3A-C
Andrea S. Brackett, WT 5D-K
Allen A. Clare, LP 2K-C
Samuel P. Delk, BR 5A-C
James H. Everett, WT10C-K
David B. Fountain, WT 6A-K
Jeremy P. Fisher, SP 3A-C
Prentice Gilbert, PSC1B-C
Kelie H. Hammond, WT 10C-K
Kelie A. Hammond, WT 10C-K
Todd E. McCarter, MP 2C-C
Donald A. Moul, WT 7B-K
Preston P. Pratt, BR 4D-C
Ronald R. Sanders II, MR 5E-C
Jeffry W. Stichler, SPB BA-K
John M. Thomas III, MR 6D-C
Josh Thomas, SP 3K-C
Kay W. Whittenburg, MR 3A-C
Dennis H. Yankee, LAB 1B-N