Memorandum from the Office of the Inspector General

September 24, 2019

Allen A. Clare, LP 2K-C
Jeremy P. Fisher, SP 3A-C

REQUEST FOR FINAL ACTION – AUDIT 2018-15530 – HYDRO GENERATION CYBERSECURITY CONTROLS

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority (TVA) Hydro Generation's cybersecurity controls. Our objective was to determine if logical, physical, and general security controls were (1) appropriately designed to reduce cybersecurity risk and (2) operating effectively.

In summary, we found that TVA generally has logical, physical, and general security controls that were appropriately designed and operating effectively to reduce cybersecurity risk. However, we found TVA had (1) a potential single point of failure that could affect TVA's ability to operate effectively in the event of a disaster, (2) not configured network devices in a consistent manner, and (3) not maintained updated network documentation. TVA is in the process of implementing a modernization project that includes system and network redundancies that would allow the secondary site to function independently from the primary site. Specifics of the identified issues 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 a debriefing on June 19, 2019.

We recommend the Vice President, Power Operations (PO):

1. Implement the modernization project plan to eliminate the potential single point of failure.

2. Create standard configurations for network devices that follow best practices.

3. Update network diagram to accurately reflect the network environment.

TVA management provided their planned actions to address the recommendations in this report. See the Appendix for TVA management's complete response.

BACKGROUND

Hydro generation accounts for 10 percent of TVA's power portfolio. Hydro assets include 29 hydro plants and one pumped storage hydroelectric plant that together house 113 power-generating units. The operation of these assets must balance multiple demands impacting the Tennessee valley rivers and their tributaries, including flood-damage control, navigation, dam safety, hydroelectric power production, recreation, water supply, and water quality.

The Hydro control system and its supporting network infrastructure provide primary operational control of TVA's hydro assets. This network is comprised of devices that allows information to flow between these assets while reducing cybersecurity risk. Power Operations manages these network devices and TVA Information Technology (IT) provides cybersecurity monitoring.

As part of our annual audit planning, we completed a threat assessment to identify cybersecurity threats that could potentially impact TVA. The potential for a cyberattack targeted on Hydro assets was one of the areas identified. Therefore, we included an audit of TVA's hydro generation cybersecurity controls as part of our 2019 audit plan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if logical, physical, and general security controls were (1) appropriately designed to reduce cybersecurity risk and (2) operating effectively. The scope of this audit was limited to the centralized Hydro control system. Our fieldwork was performed between March and June 2019. To meet our objective, we:

- Obtained and reviewed PO Standard Operating Procedure 12.100, *Hydro Generation Integrated River Operations Control System*, to gain an understanding of the system environment.
- Reviewed the results of a recent external review of the subject area.
- Reviewed network diagrams to obtain understanding of the logical network design.
- Reviewed TVA project documents regarding plans for updating Hydro network's architecture and design.
- Performed physical inspection of network equipment and setup at the primary and secondary sites.
- Obtained and reviewed network device configurations to compare them to industry best practices.[1]
- Performed network analysis for unusual traffic, malware traffic, or misconfigured traffic settings.
- Inquired of TVA personnel to identify and obtain information on TVA's controls to reduce cybersecurity risk.

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.

[1] Best practices used in the audit included benchmarks created by the Center for Internet Security, a nonprofit organization, through a collaboration of experts in the field of IT security.

FINDINGS

We found that TVA management generally has logical, physical, and general security controls that were appropriately designed and operating effectively to reduce cybersecurity risk. However, we found TVA had (1) a potential single point of failure that could affect TVA's ability to operate effectively in the event of a disaster, (2) not configured network devices in a consistent manner, and (3) not maintained updated network diagram documentation. Specifics of the identified issues 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 a debriefing on June 19, 2019.

POTENTIAL SINGLE POINT OF FAILURE

We reviewed the current logical network design and noted that, while TVA has an alternate processing facility as part of its contingency planning for the Hydro control system, it currently remains dependent upon its primary site. Further, we noted the connections between the two sites have limited redundancy should the connections fail. This design introduces a potential single point of failure that would stop the flow of information between assets on the Hydro control system. According to TVA management, business impact would be limited since the operating schedules are distributed in advance and equipment at the plants could be manually operated. However, a catastrophic event affecting the primary site could cause delayed reconnection resulting in computer equipment at both the primary and alternate sites not functioning properly. TVA is in the process of implementing a modernization project that includes system and network redundancies that would allow the secondary site to function independently from the primary site.

NETWORK DEVICE CONFIGURATION INCONSISTENT

We reviewed the configurations of nine network devices used to reduce cybersecurity risk in TVA's Hydro control system and compared them against industry best practices. We found four of the nine devices were not consistently configured in accordance with best practices. We were informed by PO that they are not required to follow any best practice standards for configuring these devices and that there is no policy in place directing them to do so. However, having a standard configuration for devices will provide a higher level of security and greater ability of knowing and tracking how each device is secured.

NETWORK DOCUMENTATION NEEDS UPDATING

We reviewed Hydro control system's network diagram and found one network device on the diagram had been decommissioned several years ago. We confirmed with TVA personnel that this device was not present on the Hydro control system network at either the primary or the secondary site.

RECOMMENDATIONS

We recommend the Vice President, Power Operations:

1. Implement the modernization project plan to eliminate the potential single point of failure.

   TVA Management's Comments – TVA management stated the modernization project will continue to 2021 and project completion will remediate this recommendation. See the Appendix for TVA management's complete response.

2. Create standard configurations for network devices that follow best practices.

   TVA Management's Comments – TVA management stated Power Operations will partner with TVA Cybersecurity and Information Technology to update TVA Standard Programs and Processes 12.704, *Security Configuration Benchmark Standards*, that will establish recommended standards and best practices to be considered for applicability to the Hydro Generation Systems. See the Appendix for TVA management's complete response.

3. Update network diagram to accurately reflect the network environment.

   TVA Management's Comments – TVA management stated that network diagram updates will be completed as part of the modernization project. See the Appendix for TVA management's complete response.

- - - - - -

Your written comments, which addressed your management decision and actions planned or taken, have been included in the Appendix. 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 findings, please contact Jonathan B. Anderson, Senior Auditor, at (865) 633-7340 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)
WT 2C-K

JBA:KDS
Attachment
cc: See page 2

cc (Attachment):
TVA Board of Directors
Clifford L. Beach Jr., WT 7B-K
Andrea S. Brackett, WT 5D-K
Robertson D. Dickens, WT 9C-K
Michael R. Holt, LP 2V-C
Jeffrey J. Lyash, WT 7B-K
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Todd E. McCarter, MP 2C-C
Stacey L. Parrott, LP 3K-C
Sherry A. Quirk, WT 7C-K
Ronald R. Sanders II, MR 5E-C
John M. Thomas III, MR 6D-C
Jacinda B. Woodward, LP 2K-C
OIG File No. 2018-15530

September 18, 2019

David P. Wheeler, WT 2C-K

REQUEST FOR COMMENTS – DRAFT AUDIT 2018-15530 – HYDRO GENERATION CYBERSECURITY CONTROLS

Mr. Wheeler,

This is in response to your memorandum dated August 22, 2019. After review of the draft audit, please see the following response to the Recommendations Hydro Generation Cybersecurity Controls.

We would like to thank Jonathan Anderson and the audit team for their diligence and support to enhance the Hydro Generation Cybersecurity controls.

Recommendations:

We recommend the Vice President, Power Operations (PO):

1. Implement the modernization project plan to eliminate the potential single point of failure.

Response
The Hydro IROCS Modernization Project was approved June 2018 and will continue to 2021. One of the project goals is to establish fully independent control centers. Completion of this project will remediate this recommendation. The completion date is dependent upon the project timeline and milestones being completed as scheduled.
Risk: Medium

2. Create standard configurations for network devices that follow best practices.

Response
Power Operations will partner with TVA Cybersecurity and Information Technology to update TVA-SPP-12.704 Security Configuration Benchmark Standards that will establish recommended standards, and best practices to be considered for applicability to the Hydro Generation Systems. Power Operations will follow the guidance and process established when the SPP is published.
Risk: Low

3. Update network diagram to accurately reflect the network environment.

Response
As part of the Hydro IROCS Modernization Project, network diagram updates will be completed. The recommended change will be completed as part of the first update to the HDCC diagram.

Thank you for allowing us to provide these comments. Please contact us if you have any questions.

Allen A. Clare
Vice President
Gas & Hydro Power Operations
LP 2K-C

Jeremy P. Fisher
Vice President
Information Technology
SP 3A-C

SAB:MPL:ALH
cc: Clifford L. Beach Jr., WT 6A-K
Andrea S. Brackett, WT 5D-K
Robertson D. Dickens, WT 9C-K
Michael R. Holt, LP 2V-C
Todd E. McCarter, MP 2C-C
Stacey L. Parrott, LP 3K-C
Sherry A. Quirk, WT 7C-K
John M. Thomas III, MR 6D-C
Jacinda B. Woodward, LP 2K-C
OIG File No. 2018-15530