Memorandum from the Office of the Inspector General

August 26, 2019

Jeremy P. Fisher, SP 3A-C
Carrie M. Fogleman, PCC 2A-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2019-15636 – TRANSMISSION SYSTEM PERIMETER ATTACKS

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority (TVA) transmission system's Internet security. Our objective was to determine if TVA could appropriately prevent, detect, and defend against cyberattacks from the Internet targeting the transmission system.

In summary, we (1) identified vulnerabilities that increase TVA's risk of successful cyberattacks, (2) found a gap in how TVA's cybersecurity monitoring system detects cyberattacks against the transmission system, (3) found TVA had not documented an automated tool within their policies and processes, and (4) found TVA had not configured network devices in a consistent manner. Specifics of the identified vulnerabilities and the corresponding devices 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 May 30, 2019.

We made several recommendations to TVA management to address the issues we identified. Subsequent to our draft audit report, management provided additional information regarding applicable policies and procedures as well as documentation of actions that had been taken to address the vulnerabilities we identified. Management's comments provided in response to our draft report referenced the subsequent information and documentation provided to us. Management agreed with our remaining recommendations. See the Appendix for TVA management's complete response.

We reviewed the documentation provided by TVA management, conducted additional analysis, and determined that TVA had remediated or mitigated all identified vulnerabilities. We also revised our report to reflect the new information provided by management.

BACKGROUND

TVA's Transmission, Power Supply and Support (TPS&S) operates TVA's power grid and acts as a balancing authority to help sustain the reliability of the Eastern Interconnect. TPS&S plans, designs, builds, operates, and maintains TVA's transmission system and works with generation partners to keep the grid balanced and reliable. TPS&S utilizes controls technologies for real-time visibility and reliable grid operations. In addition, TPS&S utilizes the Internet for nonoperation communications with external entities. Internet connectivity presents risks to organizations (e.g., TVA) that could be leveraged for unauthorized access to internal systems. TPS&S manages network devices that protect

and defend against cyberattack and TVA Information Technology (IT) provides cybersecurity monitoring for the transmission Internet connections to detect potential cyberattacks.

As part of our annual audit planning, we completed a threat assessment to identify high-risk cybersecurity threats that could potentially impact TVA. The potential for the exploitation of TVA's transmission system's Internet connectivity was one of those high-risk areas. Therefore, we included an audit of TVA transmission system's Internet security as part of our 2019 audit plan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA could appropriately prevent, detect, and defend against cyberattacks from the Internet targeting the transmission system. The scope of this audit was limited to the Internet connection managed by TPS&S. Our fieldwork was performed between March and June 2019. To meet our objective we:

- Obtained and reviewed TPS&S policies and technical procedures.
  - TVA Standard Programs and Processes (SPP) 12.006, *Cyber Incident Response*
  - Transmission Operations & Power Supply (TOPS) Central Operations & Infrastructure (COI) SPP-12.810, *Configuration Change Management and Vulnerability Assessments*
  - TOPS-COI-TP-12.836, *Firewall Security Configuration and Installation*
  - TOPS-COI-TP-12.838, *Switch and Router Security Configuration and Installation*
- Performed a gap analysis comparing TPS&S policies and technical procedures against best practices.[1]
- Obtained and reviewed network device configurations to compare them to industry best practices.[2]
- Reviewed prior work from our 2018 Federal Information Security Modernization Act[3] audit specific to TVA's incident response program to validate TVA cybersecurity incident response policies and procedures.
- Performed network penetration testing against devices accessible through the TPS&S Internet connection to identify and verify vulnerabilities.
- Inquired of TVA personnel to determine if TVA identified our penetration testing activities.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain

---

1 National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015.

2 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.

3 Audit Report 2018-15526, *2018 Federal Information Security Modernization Act*, December 18, 2018.

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 performed penetration testing and identified vulnerabilities that increase TVA's risk of successful cyberattacks. We also found a gap in how TVA's cybersecurity monitoring system detects cyberattacks against the transmission system. In addition, we found that TVA had not documented an automated tool within their policies and processes and had not configured network devices in a consistent manner. 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 a debriefing on May 30, 2019.

Vulnerabilities Identified That Increase TVA's Cyber Risk

We identified 17 communication paths used by transmission devices accessible from the Internet. We conducted penetration testing and, using various tools, tested each communication path for vulnerabilities. We found 13 of the 17 communication paths were vulnerable to cyberattack.

Subsequent to our draft audit report, TVA management informed us that the vulnerabilities identified had been addressed. We reviewed the provided documentation and conducted additional penetration testing on the communication paths, and confirmed the vulnerabilities had been remediated.

Cybersecurity Monitoring System Gap

We found a gap in TVA IT's monitoring of the transmission Internet connection. Based on the results of our penetration testing, we determined that TVA cybersecurity monitoring should have detected one of our tests. In discussions with TVA personnel, we noted the gap that prevented IT from identifying our testing.

Automated Tool Not Documented

We reviewed TVA policies and processes related to the monitoring and maintenance of the network devices used to prevent and defend against cyberattacks targeting TVA's transmission system. We noted that while TVA has documented some of the automated tools used for monitoring and maintenance of network devices, they have not documented all of the tools in place.

Subsequent to our draft audit report, TVA management provided clarification on the scope of the referenced TVA policies and procedures. We reviewed the information and concur that the referenced procedure was out of scope. Accordingly, we have removed the related recommendation.

Network Device Configuration Inconsistent

We reviewed 15 network device configurations used for Internet connectivity and cybersecurity managed by TPS&S and compared them against industry best practices. We found all 15 were not consistently configured in accordance with best practices.

RECOMMENDATIONS

We recommend the General Manager, Central Operations and Infrastructure:

1. Create baseline configurations for network devices.

We recommend the Vice President and Chief Information Officer, IT, and the General Manager, Central Operations and Infrastructure:

2. Review transmission Internet connection cyber monitoring and make improvements where possible to close the gap identified.

TVA Management's Comments - Management's comments provided in response to our draft report referenced the (1) information that had been provided to us subsequent to our draft report and (2) documentation of remediation actions that had been taken to address the identified vulnerabilities. Management also agreed with our two remaining recommendations. See the Appendix for TVA management's complete response.

Auditor's Response – We reviewed the information and clarifications provided by TVA management subsequent to our draft report date and revised our report accordingly. As stated previously, we also determined that TVA had remediated or mitigated all previously identified vulnerabilities.

- - - - - -

This report is for your review and information. Please advise us of your management decision regarding the two open recommendations 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 wish to discuss our observations, please contact Scott A. Marler, Audit Manager, at (865) 633-7352 or Sarah E. Huffman, Director, IT 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

SAM: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
James R. Dalrymple, MR 3H-C
Robertson D. Dickens, WT 9C-K
Jeffrey J. Lyash, WT 7B-K
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Todd E. McCarter, MP 2C-C
Aaron P. Melda, MR 1B-C
Sherry A. Quirk, WT 7C-K
Ronald R. Sanders II, MR 5E-C
Michael D. Skaggs, WT 7B-K
John M. Thomas III, MR 6D-C
OIG File No. 2019-15636

August 15, 2019

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2019-15636
TRANSMISSION SYSTEM PERIMETER ATTACKS

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, Scott Marler, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact John Tracy or Krystal Brandenburg.

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

Carrie Fogleman
General Manager, Central Operations and Infrastructure
Transmission, Power Supply & Support
PCC 2A-C

ASB:SLW
cc (Attachment): Response to Request
Samuel Austin, MP 3B-C
Clifford Beach, WT 7B-K
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Krystal Brandenburg, MP 2B-C
James Dalrymple, MR 3H-C
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C
Benjamin Jones, SP 3L-C
Todd McCarter, MP 2C-C
Jill Matthews, WT 2C-K
Aaron Melda, MR 1B-C
Sherry Quirk, WT 7C-K
Michael Skaggs, WT 7B-K
John Thomas, MR 6D-C
OIG File No. 2019-15636

Audit 2019-15636
Transmission System Perimeter Attacks
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Page	Draft Report Section	Comments
2	Background	Management met with the OIG and provided clarification regarding TPS&S's use of internet connectivity.
2	Objective, Scope, and Methodology	Management met with the OIG and provided clarification regarding the TPS&S policies and technical procedures referenced within the body of the report.

Recommendation		Comments
1	We recommend the General Manager, Central Operations and Infastructure: Remediate or mitigate identified vulnerabilities.	Management agrees and has provided the OIG documentation demonstrating remediation of all identified vulnerabilities.
2	Update policies to include automated tools in use.	Management provided clarification regarding the scope of SPPs reviewed during audit field work performed.
3	Create baseline configurations for network devices.	Management agrees.
4	We recommend the Vice President and Chief Information Officer, IT, and the General Manager, Central Operations and Infrastructure: Review transmission Internet connection cyber monitoring and make improvements where possible.	Management agrees.