Memorandum from the Office of the Inspector General

September 22, 2021

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2021-15777 – PRIVILEGED ACCOUNT MANAGEMENT

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority's (TVA) management of privileged accounts. Our objective was to determine if TVA's management of privileged accounts is following TVA policy and best practices. A privileged user has an account that is authorized for the performance of security-related functions that ordinary users cannot perform. Privileged account management can be defined as managing and logging account and data access by privileged users.

In summary, we found several controls of TVA's privileged account management to be generally effective, including (1) an accurate inventory of privileged network device accounts, (2) appropriate segregation of duties, (3) appropriate account lifecycle management for most privileged users, and (4) monitoring of privileged accounts. However, we also found (1) improper usage of primary user accounts with privileged access, (2) one account with inappropriate privileged access, and (3) several gaps in TVA's Standard Programs and Processes (SPP) when compared to best practices. 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 July 22, 2021.

We recommend the Vice President and Chief Information and Digital Officer, Technology and Innovation (T&I):

1. Take action to ensure primary accounts are prohibited from having privileged access as required in TVA-SPP-12.003, *IT Account Management.*

2. Implement an additional periodic review by T&I management of the privileged account inventory and assigned access.

3. Review gaps in best practices and incorporate into TVA SPPs accordingly.

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

BACKGROUND

TVA SPP 12.003, *IT Account Management*, defines privileged account as "either local or network user accounts that have escalated administrative levels of system rights and access." National Institute of Standards and Technology[1] defines a privileged user as having an account "that is authorized for the performance of security-related functions that ordinary users cannot perform, such as administrative access." The Center for Internet Security[2] (CIS) states that "the misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise." Effective privileged account management increases security by managing and logging account and data access by privileged users.

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 exploitation of privileged accounts was one of those high-risk areas. Mitigating information system controls for misuse of privileged accounts include maintaining an accurate inventory of accounts, segregation of duties, authentication, monitoring, as well as management of the account lifecycle. The resulting impact of privileged access abuse could be data loss, fraud, sabotage, theft of intellectual property, business disruption, or even reputation degradation. Therefore, we included an audit of TVA's management of privileged accounts as part of our 2021 audit plan.

During audit fieldwork, Executive Order 14028[3] was issued on May 12, 2021, which consists of 74 actionable directives that focuses on improving cybersecurity of federal systems and networks. These directives include removing barriers to threat information sharing, implementing stronger cybersecurity standards, and improving software supply chain security. While the directives are not specific to privileged account management, TVA's response to the executive order could affect this area.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA's management of privileged accounts is following TVA policy and best practices. The scope of this audit was limited to privileged accounts managed by TVA T&I. Fieldwork was performed between December 2020 and July 2021. To achieve our objective, we:

- Obtained and reviewed TVA-SPP-12.003, *IT Account Management*, and TVA's common control catalog.
- Interviewed T&I personnel and performed process walkthroughs to identify and obtain information on TVA's controls for privileged account management.

---

1 The National Institute of Standards and Technology is a physical sciences laboratory and a part of the agency of the United States Department of Commerce with a mission is to promote American innovation and industrial competitiveness

2 Center for Internet Security, a nonprofit organization, is a collaboration of experts in the field of IT security.

3 United States, Executive Office of the President [Joseph R. Biden, Jr.], Briefing Room, *Executive Order 14028 – Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>, accessed on August 02, 2021.

- Performed a gap analysis comparing TVA policies and privileged account management controls against best practices.[4]
- Identified and tested controls related to inventory, segregation of duties, account lifecycle, authentication, and monitoring.

Inventory, segregation of duties, account lifecycle management, authentication and monitoring were identified as information system controls that were significant to our audit objective. As such, they were included in our audit plan for testing. 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

FINDINGS

We found several controls of TVA's privileged account management to be generally effective, including (1) an accurate inventory of privileged network device accounts, (2) appropriate segregation of duties, (3) appropriate account lifecycle management for most privileged users, and (4) monitoring of privileged accounts. However, we also found (1) improper usage of primary accounts with privileged access, (2) one account with inappropriate privileged access, and (3) several gaps in TVA's SPPs when compared to best practices. 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 July 22, 2021.

IMPROPER USAGE OF PRIMARY ACCOUNTS FOR PRIVILEGED ACCESS

TVA-SPP 12.003 requires privileged access to be separated on a second account, rather than a user's primary account. We reviewed privileged accounts and identified 18 primary accounts with privileged access. Prior to completion of our audit, TVA T&I took action to address 2 of the 18 accounts identified; therefore, 16 primary accounts with privileged access were still active. Not maintaining separate administrative or privileged credentials can expose systems and make it easier for an attacker to gain increased control of the environment by using a primary account with privileged access.

INAPPROPRIATE PRIVILEGED ACCESS

We reviewed privileged accounts for appropriate segregation of duties and found privileged access was not completely removed when one employee was transferred out of T&I to a role in another TVA organization in 2018. A ticket had been submitted to T&I requesting access removal in 2018 but was closed before all work was completed, and the employee's current manager approved the continued access in subsequent management

[4] Best practices used in the audit included benchmarks created by CIS and NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020.

reviews. Active and unnecessary privileged access increases the risk of the account being abused by an attacker.

GAPS IN POLICY WHEN COMPARED TO BEST PRACTICES

We reviewed TVA-SPP-12.003 and privileged account management controls and compared them against best practices. We found less than half of the best practices were included in TVA-SPP-12.003 and privileged account management controls. Specifically, we identified several practices that were not reflected by current TVA documentation. The subject areas of identified gaps included (1) maintaining an inventory of administrative accounts, (2) multifactor authentication for all administrative access, and (3) documenting the process of logging privileged functions as well as other documentation gaps.

RECOMMENDATIONS

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

1. Take action to ensure primary accounts are prohibited from having privileged access as required in TVA-SPP-12.003.

2. Implement an additional periodic review by T&I management of the privileged account inventory and assigned access.

3. Review gaps in best practices and incorporate into SPP policies accordingly.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendations. 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 Megan E. Spitzer, Senior Auditor, at (865) 633-7394 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.

Curtis C Hudson

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

MES:KDS
cc: See page 5

cc: TVA Board of Directors
Douglas R. Biederman
Andrea S. Brackett
Richard E. Conyer
Buddy Eller
David Fountain
David M. Harrison
Greg G. Jackson
Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Lindsey M. Stewart
John M. Thomas III
OIG File No. 2021-15777

September 17, 2021

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2021-15777 – PRIVILEGED ACCOUNT 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, Megan Spitzer, 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
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. 2021-15777

Audit 2021 - 15777
PRIVILEGED ACCOUNT MANAGMENT
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: Take action to ensure primary accounts are prohibited from having privileged access as required in TVA-SPP-12.003.	Management Agrees
2	Implement an additional periodic review by T&I management of the privileged account inventory and assigned access.	Management Agrees
3	Review gaps in best practices and incorporate into SPP policies accordingly.	Management Agrees