



Memorandum from the Office of the Inspector General

November 10, 2021

Jeremy P. Fisher
Michael S. Turnbow

FINAL REPORT – AUDIT 2020-15723 – TVA’S INTERNET PERIMETER

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority’s (TVA) Internet perimeter. Our objective was to identify cybersecurity weaknesses in TVA’s Internet perimeter through penetration testing.

In summary, we identified some vulnerabilities in TVA’s internet perimeter. Specifically, we (1) downloaded files related to TVA’s disposal of coal ash that were marked as confidential, (2) accessed a Web site related to river operations that used weak authentication, and (3) found TVA’s password complexity requirements on a TVA publicly available Web site. Specifics of the identified vulnerabilities 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 briefings on August 23 and 24, 2021.

We recommend the Vice President (VP), Civil Projects and Equipment Support Services (ESS)/Coal Combustion Products (CCP):

1. Ensure that documents related to TVA’s disposal of coal ash for public release are properly reviewed and TVA information classification markings removed.

In response to our draft report and based on discussions with TVA Office of General Counsel, TVA management disagreed with this recommendation, as it could negatively affect public perception and reputation by altering previously posted public facing compliance documents. However, management stated that future public facing documents will be reviewed for TVA classification markers and removed if deemed appropriate. See Appendix A for TVA ESS/CCP management’s complete response. We agree with TVA management’s planned action and no further action is required.

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

2. Web sites follow TVA policy for authentication.
3. Removal of TVA’s password complexity rules from TVA’s publicly accessible Web sites.

In response to our draft report, TVA management agreed with our recommendations and stated actions to address the recommendations have been completed. See Appendix B for TVA T&I management's complete response. We verified TVA management's actions to address the recommendations have been completed and no further action is required.

BACKGROUND

TVA utilizes Internet-accessible systems to provide public information, employee services, and some business functions. Internet-accessible systems present risks to organizations as they may be leveraged to access internal systems and/or confidential and sensitive information. Examples of this include the Colonial Pipeline ransomware attack and various United States Federal Agencies that have been compromised.

As part of our annual audit planning, a threat assessment was completed to identify cybersecurity high-risk areas that could potentially impact TVA. The assessment also included results from TVA's enterprise risk management process. The potential for the exploitation of Internet-accessible services to gain access to TVA's confidential and sensitive systems and data was one of those high-risk areas. Therefore, we included an audit of TVA's Internet-accessible systems to identify cybersecurity weaknesses using penetration testing methodologies.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to identify cybersecurity weaknesses in TVA's Internet perimeter through penetration testing. The scope of this audit was limited to systems managed by TVA T&I and hosted on TVA-owned servers and networks. Fieldwork was performed from December 2020 to August 2021. To meet our objective we:

- Identified Internet-accessible systems providing Web site and other services from the Internet.
- Performed penetration testing using industry standard tools to identify vulnerabilities and determine if TVA's confidential or sensitive systems and/or information could be accessed from the Internet.

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 conducted penetration testing using industry standard tools and methods and identified some vulnerabilities in TVA's Internet perimeter. Specifically, we (1) downloaded files related to TVA's disposal of coal ash that were marked as confidential, (2) accessed a Web site related to river operations that used weak

authentication, and (3) found TVA's password complexity requirements on a TVA publicly available Web site.

DOCUMENTS MARKED AS TVA CONFIDENTIAL ACCESSIBLE FROM THE INTERNET

We found an application interface that allowed unauthenticated access and downloaded 1,072 documents related to TVA's disposal of coal ash. Based on document title, we reviewed seven of these documents and noted that sections of the documents were marked "TVA Confidential Information." According to TVA management, the documents in question were made available to the public pursuant to the Resource Conservation and Recovery Act¹ and should have had the "TVA Confidential Information" marking removed. We noted TVA has a reputational risk in that someone could download these documents and claim they have accessed TVA's confidential information related to coal ash disposal.

WEB SITE WITH WEAK AUTHENTICATION

We found a Web site that used weak authentication for access and were able to log into the Web site and view information related to TVA's river operations. After reviewing and discussing the information with TVA, we determined this was low risk as much of the information is publicly available through other TVA sources. However, we noted TVA has a reputational risk in that someone could inappropriately access this site and publicly claim they have hacked TVA and retrieved river operations operational data.

TVA PASSWORD COMPLEXITY REQUIREMENTS ACCESSIBLE FROM THE INTERNET

We found TVA's password complexity requirements on a TVA Web site that is available to the public. This information can be used to create lists of possible passwords for conducting authentication attacks against TVA's resources increasing the probability of gaining inappropriate access.

RECOMMENDATIONS

We recommend the VP, Civil Projects and ESS/CCP:

1. Ensure that documents related to TVA's disposal of coal ash for public release are properly reviewed and TVA information classification markings removed.

TVA Management's Comments – In response to our draft report and based on discussions with TVA Office of General Counsel, TVA management disagreed with this recommendation, as it could negatively affect public perception and reputation by altering previously posted public facing compliance document. However, management stated that future public facing documents will be reviewed for TVA classification

¹ The Resource Conservation and Recovery Act gives the Environmental Protection Agency the authority to control hazardous waste from cradle to grave. This includes the generation, transportation, treatment, storage, and disposal of hazardous waste.

markers and remove if deemed appropriate. See Appendix A for TVA ESS/CCP management's complete response.

Auditor's Response – We agree with TVA management's planned actions and no further action is required.

We recommend the VP and Chief Information and Digital Officer, T&I, ensure:

2. Web sites follow TVA policy for authentication.
3. Removal of TVA's password complexity rules from TVA's publicly accessible Web sites.

TVA Management's Comments – In response to our draft report, TVA management agreed with these recommendations and stated actions to address the recommendations have been completed. See Appendix B for TVA T&I management's complete response.

Auditor's Response – We verified TVA management's actions to address the recommendations have been completed and no further action is required.

- - - - -

This report is for your review and information. No response to this report is necessary. If you have any questions, 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
Andrea S. Brackett
Robert M. Deacy Sr.
Samuel P. Delk
Buddy Eller
Gregory G. Jackson
David B. Fountain
Tracy E. Hightower

Jeffrey J. Lyash
Jill M. Matthews
Todd E. McCarter
Donald A. Moul
Ronald R. Sanders II
John M. Thomas III
Joshua R. Thomas
Kay W. Whittenburg
OIG File No. 2020-15723

October 29, 2021

David P. Wheeler, WT 2C-K

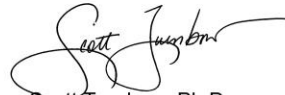
RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2020-15723 – TVA
INTERNET PERIMETER

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 Brandy Barbee.



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



Scott Turnbow, Ph.D.
Vice President and Civil Projects
and Equipment Support Services/
Coal Combustion Products
LP 5D-C

ASB:BAB
cc (Attachment): Response to Request
Brandy Barbee, MP 2B-C
Brett Atkins
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Robert Deacy Sr. LP 5D-C
David Fountain, WT 6A-K
David Harrison, MP 5C-C
Tracy Hightower, LP 5B-C

Gregory Jackson
Benjamin Jones, SP 3L-C
Todd McCarter, MP 2C-C
Don Moul, WT 7B-K
Ronald Sanders, MR 5E-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2020-15723

Audit 2020-15723
TVA Internet Perimeter
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	We recommend the Vice President (VP), Civil Projects and Equipment Support Services (ESS)/Coal Combustion Products (CCP): Ensure that documents related to TVA's disposal of coal ash for public release are properly reviewed and TVA information classification markings removed.	Based on discussions with OGC, management disagrees with the recommendation, as it could negatively affect public perception and reputation by altering previously posted public facing compliance documents. Management will ensure that future public facing documents are reviewed for TVA classification markings and removed if deemed appropriate.
2	We recommend the VP and Chief Information and Digital Officer, Technology and Innovation (T&I): Ensure websites follow TVA policy for authentication.	Management agrees.
3	We recommend the VP and Chief Information and Digital Officer, Technology and Innovation (T&I): Ensure removal of TVA's password complexity rules from TVA's publicly accessible Web sites.	Management agrees.

November 4, 2021

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2020-15723 – TVA
INTERNET PERIMETER

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 Brandy Barbee.



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

Michael Turnbow
Vice President and Civil Projects
and Equipment Support Services/
Coal Combustion Products
LP 5D-C

ASB:BAB
cc (Attachment): Response to Request
Brandy Barbee, MP 2B-C
Brett Atkins
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Robert Deacy Sr. LP 5D-C
David Fountain, WT 6A-K
David Harrison, MP 5C-C
Tracy Hightower, LP 5B-C

Gregory Jackson
Benjamin Jones, SP 3L-C
Todd McCarter, MP 2C-C
Don Moul, WT 7B-K
Ronald Sanders, MR 5E-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2020-15723

Audit 2020-15723
TVA Internet Perimeter
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	<p>We recommend the Vice President (VP), Civil Projects and Equipment Support Services (ESS)/Coal Combustion Products (CCP):</p> <p>Ensure that documents related to TVA's disposal of coal ash for public release are properly reviewed and TVA information classification markings removed.</p>	<p>Based on discussions with OGC, management disagrees with the recommendation, as it could negatively affect public perception and reputation by altering previously posted public facing compliance documents. Management will ensure that future public facing documents are reviewed for TVA classification markings and removed if deemed appropriate.</p>
2	<p>We recommend the VP and Chief Information and Digital Officer, Technology and Innovation (T&I):</p> <p>Ensure websites follow TVA policy for authentication.</p>	<p>Management agrees and the actions have been completed for this recommendation.</p>
3	<p>We recommend the VP and Chief Information and Digital Officer, Technology and Innovation (T&I):</p> <p>Ensure removal of TVA's password complexity rules from TVA's publicly accessible Web sites.</p>	<p>Management agrees and the actions have been completed for this recommendation.</p>