



Memorandum from the Office of the Inspector General

August 22, 2018

Jeremy P. Fisher, MP 3B-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2018-15545 – TVA’S SERVER OPERATING SYSTEM BASELINES

As part of our annual audit plan, we audited the Tennessee Valley Authority’s (TVA) server operating system baselines. Our objective was to determine if TVA’s baselines are in alignment with best practices.

We reviewed TVA’s three operating system baselines and how they are applied to the tools used to deploy and manage TVA systems. In summary, we found TVA management aligned two of the three server operating system baselines with the identified best practices and had documentation to support any deviations. However, we found one of the three operating system baselines did not fully align with the identified best practices and was not completely applied to the tools used to deploy and manage server configurations. 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 debriefing on June 22, 2018. We recommend the Director, Information Technology (IT) Planning and Operations, take action to align TVA’s server operating system baselines with industry best practices and apply those baselines to the tools used for the deployment and ongoing configuration management of TVA’s servers. TVA management agreed with the audit findings and recommendation in this report. See the Appendix for TVA management’s complete response.

BACKGROUND

Standard configurations, or baselines, for server operating systems help provide a secure and consistent server environment across an enterprise. Enterprises develop these baselines based on known risks, industry best practices, and the operational needs of their individual computing environments. TVA developed three baselines for server operating systems for use within its environment and uses them during the deployment and ongoing management of server configurations. In previous audits, we compared system configurations with TVA’s established baselines. As part of our 2018 annual audit plan, we included this audit to evaluate TVA’s server operating system baselines alignment with best practices.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if the baselines are in alignment with identified best practices. The audit scope included operating system baselines for servers deployed and maintained by TVA's IT. Fieldwork was performed between April 2018 and June 2018. To achieve our objective, we:

- Reviewed TVA's Standard Program and Process 12.704, *Security Configuration Benchmark Standards*, to identify in-scope server operating systems and applicable best practices.
- Interviewed IT personnel to identify and obtain information on TVA's operating systems and their baselines.
- Obtained TVA's operating system baselines and compared them to best practices¹ to determine if they were properly aligned.
- Obtained and reviewed documentation for deviations from best practices.
- Performed walkthroughs of relevant tools used during the provisioning and configuration management processes that utilize the server operating system baselines.

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 reviewed TVA's three operating system baselines and how they are applied to the tools used to deploy and manage TVA systems. In summary, we found TVA management aligned two of the three server operating system baselines with the identified best practices and had documentation to support any deviations. However, we found one of the three server operating system baselines did not fully align with the identified best practices and was not completely applied to the tools used to deploy and manage TVA server configurations. 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 debriefing on June 22, 2018.

BASELINE NOT FULLY ALIGNED WITH BEST PRACTICES

We compared the three server operating system baselines against best practices and noted one baseline was not properly aligned. Specifically, we noted 11 deviations from best practice benchmarks, 3 that did not have documented exceptions and 8 benchmarks that were inaccurately documented by TVA. Deviations from the best practice benchmarks should be properly documented and include how TVA is addressing the related risk of potential vulnerabilities and exposures.

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.

BASELINE NOT FULLY APPLIED TO SERVER DEPLOYMENT AND MANAGEMENT TOOLS

We reviewed tools used to deploy and manage the three server operating system configurations and noted one of the three baselines was not fully applied. Tools that do not apply all aspects of a baseline can increase risk for vulnerabilities and exposures.

RECOMMENDATION

We recommend the Director, IT Planning and Operations, take action to align TVA's server operating system baselines with industry best practices and apply those baselines to the tools used for the deployment and ongoing configuration management of TVA's servers.

TVA Management's Comments – TVA management agreed with the audit findings and recommendation in this report. See the Appendix for TVA management's complete response.

- - - - -

This report is for your review and management decision. Please advise us of your management decision within 60 days from the date of this report. Information contained in this report will be subject to public disclosure. 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
Assistant Inspector General
(Audits and Evaluations)
WT 2C-K

SAM:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
David M. Harrison, MP 5C-C
William D. Johnson, WT 7B-K

Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Philip D. Propes, MP 2C-C
John M. Thomas III, MR 6D-C
OIG File No. 2018-15545

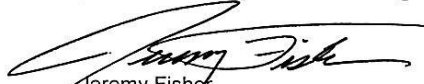
August 20, 2018

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2018-15545 – TVA'S
OPERATING SYSTEM BASELINES

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 Krystal Brandenburg.



Jeremy Fisher
Director, IT Planning & Operations
Information Technology
MP 3B-C

cc (Attachment):

James Berrong, MR 3M-C
Andrea Brackett, WT 5D-K
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C

Dwain Lanier, MR 6D-C
Jill Matthews, ET 4C-K
Philip Propes, MP 2B-C
John Thomas III, MR 6D-C
OIG File No. 2018-15545

AUDIT 2018-15545
TVA's Server Operating System Baselines
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

	Recommendation	Comments
1	We recommend the Director, IT Planning and Operations, take action to align TVA's server operating system baselines with industry best practices and apply those baselines to the tools used for the deployment and ongoing configuration management of TVA's servers.	Management agrees.