Memorandum from the Office of the Inspector General

August 16, 2017

Scott D. Self, SP 3A-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2017-15450 – TVA INTERNET-ACCESSIBLE WEB SITES

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority (TVA) Internet-accessible Web sites. Our objective was to identify cyber security weaknesses in TVA Internet-accessible Web sites through penetration testing.

In summary, 37 Internet-accessible Web sites were tested, and seven high risk vulnerabilities were identified. Two of the high risk vulnerabilities that were identified require additional testing by TVA's Information Technology (IT) for confirmation. Specifics of the identified vulnerabilities and their corresponding Web sites have been omitted from this report due to their sensitive nature in relation to TVA's cyber security but were formally communicated to TVA's IT in a debriefing on June 29, 2017. We recommend the Vice President and Chief Information Officer, IT, ensure the identified vulnerabilities are tested and remediated as appropriate. TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

BACKGROUND

TVA utilizes Internet-accessible Web sites to provide public information, employee services, and some business functions. Internet-accessible Web sites present risks to organizations as they may be leveraged to access internal systems and/or confidential and sensitive information. Examples of this include the Office of Management and Budget breach of 2016, the Ukrainian blackouts of 2015 and 2017, and many other highly publicized events.

As part of our annual audit planning, a threat assessment was completed to identify cyber security high risk areas that could potentially impact TVA. The assessment also included TVA's Enterprise Risk Assessment. The potential for the exploitation of Internet-accessible Web sites to gain access to TVA confidential and sensitive systems and data was one of those high risk areas. Therefore, we included an audit for TVA Internet-accessible Web sites in the fiscal year 2017 Audit and Evaluation Workplan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to identify cyber security weaknesses in TVA Internet-accessible Web sites through penetration testing. The scope of this audit was limited to Web sites hosted on TVA-owned servers and networks. Fieldwork was performed during May and June of 2017. To meet our objective, the audit team identified 37 TVA Internet-accessible

Web sites, tested each Web site for potential vulnerabilities, and performed evaluations of potential high risk vulnerabilities to confirm their existence.

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 identified 37 Internet-accessible Web sites for testing and, using various tools, tested each site for high risk vulnerabilities. We identified seven high risk vulnerabilities and confirmed their existence. Two of the high risk vulnerabilities identified require additional testing by TVA's IT for confirmation. Specifics of the identified vulnerabilities and their corresponding Web sites have been omitted from this report due to their sensitive nature in relation to TVA's cyber security but were formally communicated to TVA's IT in a debriefing on June 29, 2017. Following the debrief, TVA's IT informed us remediation plans are underway to address these vulnerabilities.

RECOMMENDATION

We recommend the Vice President and Chief Information Officer, IT, ensure the identified vulnerabilities are tested and remediated as appropriate.

TVA Management's Comments – TVA management agreed with the audit findings and recommendations in this report. 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. Information contained in this report will be subject to public disclosure. If you have any questions, please contact Scott A. Marler, Director (Acting), IT Audits, at (865) 633-7352 or Curtis C. Hudson, Deputy Assistant Inspector General, Audits, at (865) 633-7344. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)
ET 3C-K

SAM:BSC
Attachment
cc: See page 2

cc (Attachment):
TVA Board of Directors
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Clay Deloach, Jr., SP 3L-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MR 6D-C
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Melissa A. Livesey, WT 5B-K
Justin C. Maierhofer, WT 7B-K
Richard W. Moore, ET 4C-K
Philip D. Propes, MP 2C-C
John M. Thomas III, MR 6D-C
OIG File No. 2017-15450

August 11, 2017

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2017-15450 - TVA'S INTERNET- ACCESSIBLE WEB SITES

Our response to your request for comments regarding the findings of 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 Scott Marler and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg at (423) 751-6039.

Scott D. Self
Chief Information Officer
Information Technology
SP 3A-C

cc (Attachment):
Andrea S. Brackett, WT 5D-K
Krystal R. Brandenburg, MP 3C-C
Patrick Y. Buchanan, WT 5D-K
Clay Deloach, Jr., SP 3L-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MR 6D-C
Dwain K. Lanier, MR 6D-C
Richard Moore, ET 4C-K
Philip D. Propes, MP 2B-C
John M. Thomas III, MR 6D-C
OIG File No. 2017-15450

DRAFT AUDIT 2017-15450
TVA's Internet-Accessible Web Sites
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

	Recommendation	Comments
1	Recommend that the Vice President and Chief Information Officer, IT, ensure the identified vulnerabilities are tested and remediated as appropriate.	Management agrees.