Memorandum from the Office of the Inspector General

May 29, 2019

Jeremy P. Fisher, SP 3A-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2018-15607 – ENHANCED E-MAIL AND WEB SECURITY COMPLIANCE

As a part of our annual audit plan, we audited Tennessee Valley Authority's (TVA) compliance with two federal directives that require Web site and e-mail security controls for federal agencies. Our objective was to determine TVA's compliance with Office of Management and Budget's (OMB) memorandum (M) 15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, and Department of Homeland Security's (DHS) binding operational directive (BOD) 18-01, *Enhance E-mail and Web Security*, regarding Web site and e-mail security practices.

We reviewed TVA's internet domains and publicly accessible Web sites and determined TVA was not in compliance with OMB M-15-13 and DHS BOD-18-01. In addition, we found TVA's Web site inventory was incomplete. 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 March 26, 2019.

We recommend the Vice President and Chief Information Officer, Information Technology:

1. Update e-mail security policies for domains that were not compliant with DHS BOD-18-01 requirements, and review on a periodic basis for compliance.

2. Update websites that were not compliant with OMB M-15-13 and DHS BOD-18-01 requirements, and review on a periodic basis for compliance.

3. Review website inventory on a periodic basis for accuracy and completeness.

TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

BACKGROUND

During our annual audit planning, we identified two federal directives applicable to TVA that established Web site and e-mail requirements to protect user data. These directives, OMB M-15-13 and DHS BOD-18-01, require Web site and e-mail security controls for federal agencies. OMB M-15-13 requires all federal civilian publicly accessible Web sites to only provide service through a secure connection. DHS BOD-18-01 reinforces the OMB requirements with additional details and added security requirements for e-mail services. See Table 1 on the following page for requirement and deadline information.

Directive	Area of Focus	Requirement	Deadlines
OMB M-15-13	Web site Security	Provide a secure connection for all federal public Web sites that encrypts information sent between a browser or service and the user.	December 31, 2016
DHS BOD-18-01	Web site Security	Reinforce requirements described in OMB M-15-13. Remove support for weaker encryption protocols.	February 13, 2018
	E-mail Security	Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies to reduce the risk of attacks from unauthorized e-mail senders.	October 16, 2018
	Reporting Requirements	Provide DHS with Plan of Action that includes information on the current and planned implementation of the requirements.	Ongoing

Table 1

In addition, DHS BOD-18-01 included requirements to enable security measures and remove support for weaker encryption protocols for e-mail servers. However, these requirements were determined out of scope for this audit, as TVA does not have publicly accessible e-mail servers.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine TVA's compliance with OMB M-15-13 and DHS BOD-18-01, regarding Web site and e-mail security practices. The scope of this audit was limited to TVA's publicly accessible Web sites and e-mail servers. Our fieldwork was performed between November 2018 and March 2019. To achieve our objective we:

- Discussed audit procedures with Department of Interior Office of the Inspector General regarding an audit of similar scope conducted in July 2018.[1]
- Identified TVA's publicly accessible Web sites and e-mail servers through the use of tools and techniques.
- Obtained and reviewed TVA's Web site inventory from TVA Cybersecurity personnel and compared it to the population of identified publicly accessible Web sites.
- Obtained and reviewed internet domain listing provided by TVA Cybersecurity personnel.
- Scanned the population of identified publicly accessible Web sites and internet domains using tools and other techniques to determine compliance with OMB M-15-13 and DHS BOD-18-01 requirements.
- Conducted analysis to verify scan results, including corroboration with TVA personnel.
- Obtained and reviewed TVA's Agency Plan of Action to determine compliance with DHS BOD-18-01 reporting requirements.

[1] Final Inspection Report No. 2018-ITA-019, *The Department of Interior Generally Complied with Email and Web Security Mandates*, July 26, 2018.

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 reviewed TVA's internet domains and publicly accessible Web sites and determined TVA was not in compliance with OMB M-15-13 and DHS BOD-18-01. In addition, we found that TVA's Web site inventory was incomplete. We determined that TVA met the reporting requirements noted in DHS BOD-18-01 in the Agency Plan of Action. 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 March 26, 2019.

TVA WAS NOT COMPLIANT WITH OMB M-15-13 AND DHS BOD-18-01

We identified 116 TVA registered internet domains for testing e-mail security requirements. We reviewed security policies to assess compliance of the e-mail security requirements defined in DHS BOD-18-01. We found DMARC policies for 115 of the 116 domains were not in compliance. DMARC policies reduce the risk of attacks from unauthorized e-mail senders, such as phishing.

We identified 55 TVA Web sites accessible from the internet. We reviewed settings for each Web site to assess compliance of the encryption requirements defined in OMB M-15-13 and DHS BOD-18-01. We found encryption settings for 20 of the 55 Web sites were not in compliance. The requirements for the use of encrypted communications protect the data in transit between a Web site or service and the user.

WEB SITE INVENTORY IS INCOMPLETE

TVA Cybersecurity personnel maintain a manual listing of TVA's publicly accessible Web sites. Based on our testing, we identified 55 TVA Web sites accessible from the internet. During our analysis, we determined 11 of the 55 identified Web sites were not included in TVA's Web site inventory. An incomplete inventory increases the risk of controls not being applied appropriately or consistently that could result in unsecure Web sites.

RECOMMENDATIONS

We recommend the Vice President and Chief Information Officer, Information Technology:

1. Update DMARC policies for domains that were not compliant with DHS BOD-18-01 requirements and review on a periodic basis for compliance.

2. Update Web sites that were not compliant with OMB M-15-13 and DHS BOD-18-01 requirements and review on a periodic basis for compliance.

3. Review Web site inventory on a periodic basis for accuracy and completeness.

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 management decision. Please advise us of your management decision within 60 days from the date of this report. If you have any questions, please contact Weston J. Shepherd, Auditor, at (865) 633-7386 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)
WT 2C-K

WJS:KDS
cc: TVA Board of Directors
Clifford L. Beach Jr., WT 7B-K
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
Dwain K. Lanier, MR 6D-C
Melissa A. Livesey, WT 5B-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
Sherry A. Quirk, WT 7C-K
John M. Thomas III, MR 6D-C
Rebecca C. Tolene, WT 7B-K
OIG File No. 2018-15607

May 24, 2019

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2018-15607 – ENHANCED E-MAIL AND WEB SECURITY COMPLIANCE

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, Weston Shepherd, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg.

Jeremy Fisher
Vice President and Chief Information Officer
Information Technology
SP 3L-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
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C
Benjamin Jones, SP 3L-C
Dwain Lanier, MR 6D-C
Melissa Livesey, WT 5B-K
Todd McCarter, MP 2C-C
Sherry Quirk, WT 7C-K
John Thomas, MR 6D-C
Rebecca Tolene, WT 7B-K
OIG File No. 2018-15607

AUDIT 2018-15607
Enhanced E-Mail and Web Security Compliance
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	Update DMARC policies for domains that were not compliant with DHS BOD-18-01 requirements and review on a periodic basis for compliance.	Management agrees.
2	Update Web sites that were not compliant with OMB M-15-13 and DHS BOD-18-01 requirements and review on a periodic basis for compliance.	Management agrees.
3	Review Web site inventory on a periodic basis for accuracy and completeness.	Management agrees.