Memorandum from the Office of the Inspector General

November 14, 2018

Andrea S. Brackett, WT 5D-K
Jeremy P. Fisher, MP 3B-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2018-15529 – RANSOMWARE

As part of our annual audit plan, we audited the Tennessee Valley Authority's (TVA) controls for ransomware. Our objective was to determine if TVA has appropriate controls in place to prevent, detect, and respond to ransomware incidents.

We reviewed TVA's ransomware controls for one system, categorized as high risk, containing sensitive data. In summary, we found TVA management generally has appropriate controls in place to prevent, detect, and respond to a ransomware incident. However, for the selected system, we found inappropriate administrative access. To strengthen access controls, TVA currently has an ongoing Privileged Identity Management project to identify, track, and monitor administrative accounts, which is expected to be complete in 2020. In addition, we found improvements were needed in the Ransomware Incident Action Plan. Accordingly, TVA's Cybersecurity updated the Ransomware Incident Action Plan during our audit. 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 August 28, 2018.

We recommend the Director, Information Technology (IT) Planning and Operations, ensure the identified administrative and system accounts are reviewed and disabled as appropriate. We also recommend the Director, TVA Cybersecurity, complete planned actions in the Privileged Identity Management project to identify, track, and monitor privileged accounts for all systems. TVA management agreed with the audit findings and recommendations in this report. See the Appendix for TVA management's complete response.

BACKGROUND

Ransomware is the fastest growing malware threat in the business sector. This form of malware targets critical data and systems for the purpose of extortion by locking the user out of the data or system. After the user has been locked out of the data or system, the attacker demands a ransom payment. If payment is made, the attacker will purportedly provide an avenue to the victim to regain access to the system or data. Ransomware targets home users, businesses, and government networks. It can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.

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 ransomware to lock TVA users out of TVA sensitive systems and data was one of those high-risk areas. Therefore, we included an audit of ransomware as part of our 2018 audit plan.

<u>OBJECTIVE, SCOPE, AND METHODOLOGY</u>

Our objective was to determine if TVA has appropriate controls in place to prevent, detect, and respond to ransomware incidents. The scope of this audit included servers on TVA's internal network. Our fieldwork was performed between March 2018 and September 2018. To achieve our objective, we:

- Reviewed TVA Standard Programs and Processes (SPP), including:
    - TVA-SPP-12.003, *IT Account Management*, to identify access controls for administrative accounts.
    - TVA-SPP 12.004, *TVA Cybersecurity Patch and Vulnerability Management Program*, to identify patching processes.
    - TVA-SPP 12.06.02, *Cyber Incident Action Plan in Response to a Cyber Crime*,[1] to identify response plans in place for ransomware.
    - IT-SPP 12.12.019, *Manage Data*,[2] to identify processes for backups.
- Interviewed IT personnel to identify and obtain information on TVA's controls to prevent, detect, and respond to ransomware incidents.
- Identified and tested controls in place to prevent, detect, and respond to ransomware incidents, using a best practice as criteria.[3]
- Reviewed TVA's Ransomware Incident Action Plan and compared it against the best practice to determine if they were properly aligned.
- Identified a population of three systems TVA categorized as high risk and judgmentally selected one for testing based on potential impact if subject to a ransomware incident. Since this was a judgmental sample, the results of the sample cannot be projected to the population.

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.

[1] According to TVA personnel, this SPP was cancelled during our audit, effective May 17, 2018.

[2] According to TVA personnel, as of September 13, 2018, this SPP was under review.

[3] Best practice used in the audit is a United States Government interagency technical guidance document on the prevention and response to ransomware incidents.

FINDINGS

We reviewed TVA's ransomware controls for one system, categorized as high risk, containing sensitive data. In summary, we found TVA management generally has appropriate controls in place to prevent, detect, and respond to a ransomware incident. However, for the selected system, we found inappropriate administrative access. In addition, we found improvements were needed in the Ransomware Incident Action Plan. TVA's Cybersecurity updated the Ransomware Incident Action Plan during our audit. 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 August 28, 2018.

PREVENTIVE CONTROLS FOR ADMINISTRATIVE ACCESS NEED IMPROVEMENT

Preventive controls for a ransomware incident include appropriate patching, up-to-date antivirus, and appropriate access control. We reviewed the preventive controls for the selected system and found the associated server was appropriately patched and had current antivirus signatures. However, we found inappropriate administrative access. Specifically, we found:

- Three active administrative accounts that should have been disabled because the users of the accounts no longer required the level of access or are no longer employed at TVA.
- Two system accounts no longer in use that should have been disabled.
- Three system accounts that may no longer be required need to be reviewed to determine appropriateness.

If compromised, administrative and system accounts allow ransomware access to larger amounts of critical and sensitive data. To strengthen access controls, TVA currently has an ongoing Privileged Identity Management project to identify, track, and monitor administrative accounts, which is expected to be completed in 2020.

CONTROLS IN PLACE TO RESPOND TO RANSOMWARE INCIDENT

Controls to respond to a ransomware incident include maintaining current backups and incident action plans. We reviewed backup controls for the selected system's associated server and found backups were being completed in accordance with IT-SPP-12.12.019. Additionally, we compared TVA's Ransomware Incident Action Plan to an identified best practice. We found the Ransomware Incident Action Plan did not include instructions for changing passwords and deleting registry values following an incident, as recommended in the best practice. Not changing passwords or deleting registry keys following an incident can leave a system vulnerable to additional attack and expose other systems to the same attack. During the audit, we informed TVA Cybersecurity personnel of this process gap, and they updated the Ransomware Incident Action Plan to include steps to change passwords and delete registry values.

RECOMMENDATIONS

1. We recommend the Director, IT Planning and Operations, ensure the identified administrative and system accounts are reviewed and disabled as appropriate.

2. We recommend the Director, TVA Cybersecurity, complete planned actions in the Privileged Identity Management project to identify, track, and monitor privileged accounts for all systems.

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.

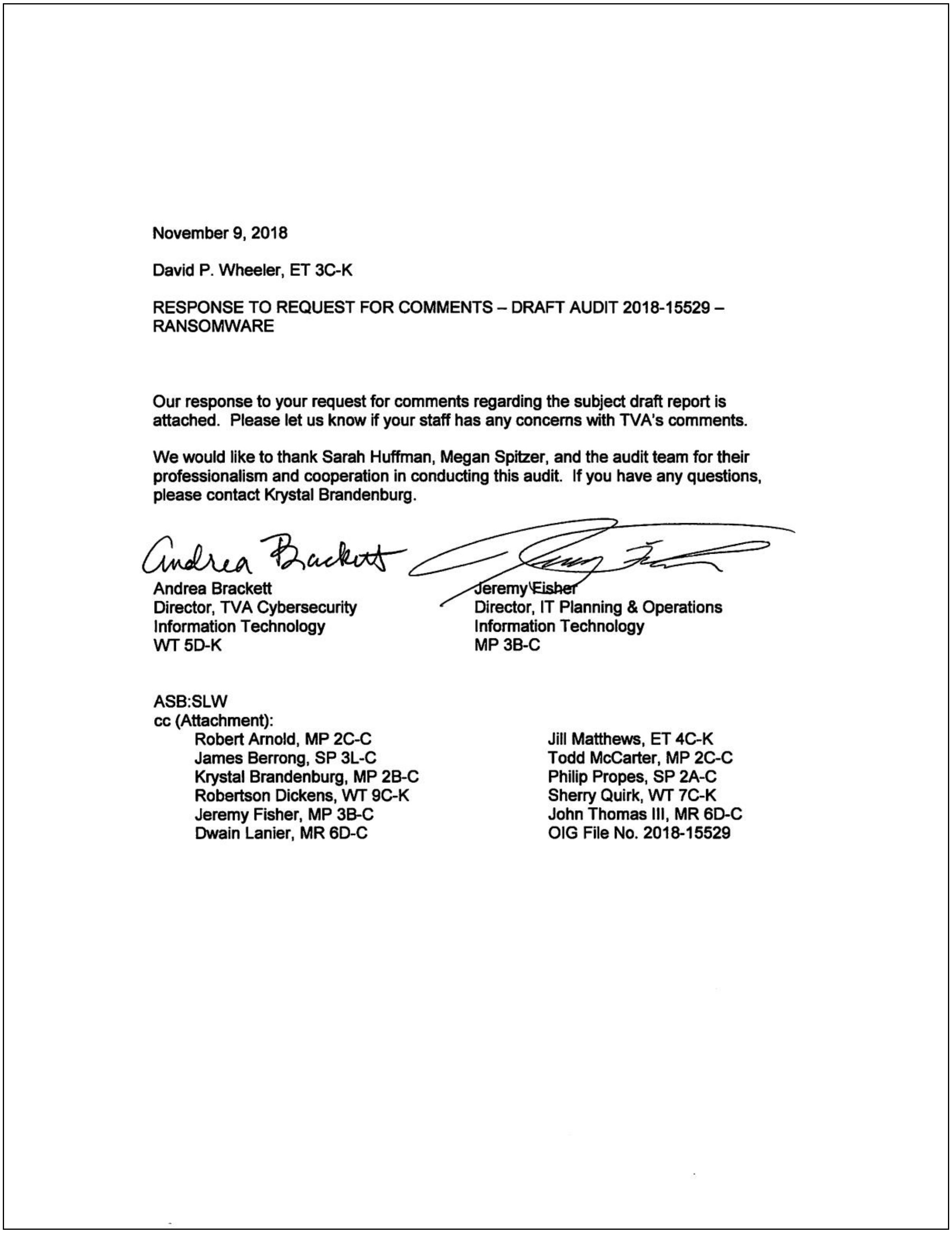
- - - - - -

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 Megan E. Spitzer, Auditor, at (865) 633-7394 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

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)
WT 2C-K

MES:KDS
cc (Attachment):
TVA Board of Directors
Robert P. Arnold, MP 2C-C
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Todd E. McCarter, MP 2C-C
Phillip D. Propes, SP 2A-C
Sherry A. Quirk, WT 7C-K
John M. Thomas III, MR 6D-C
OIG File No. 2018-15529



November 9, 2018

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2018-15529 – RANSOMWARE

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.

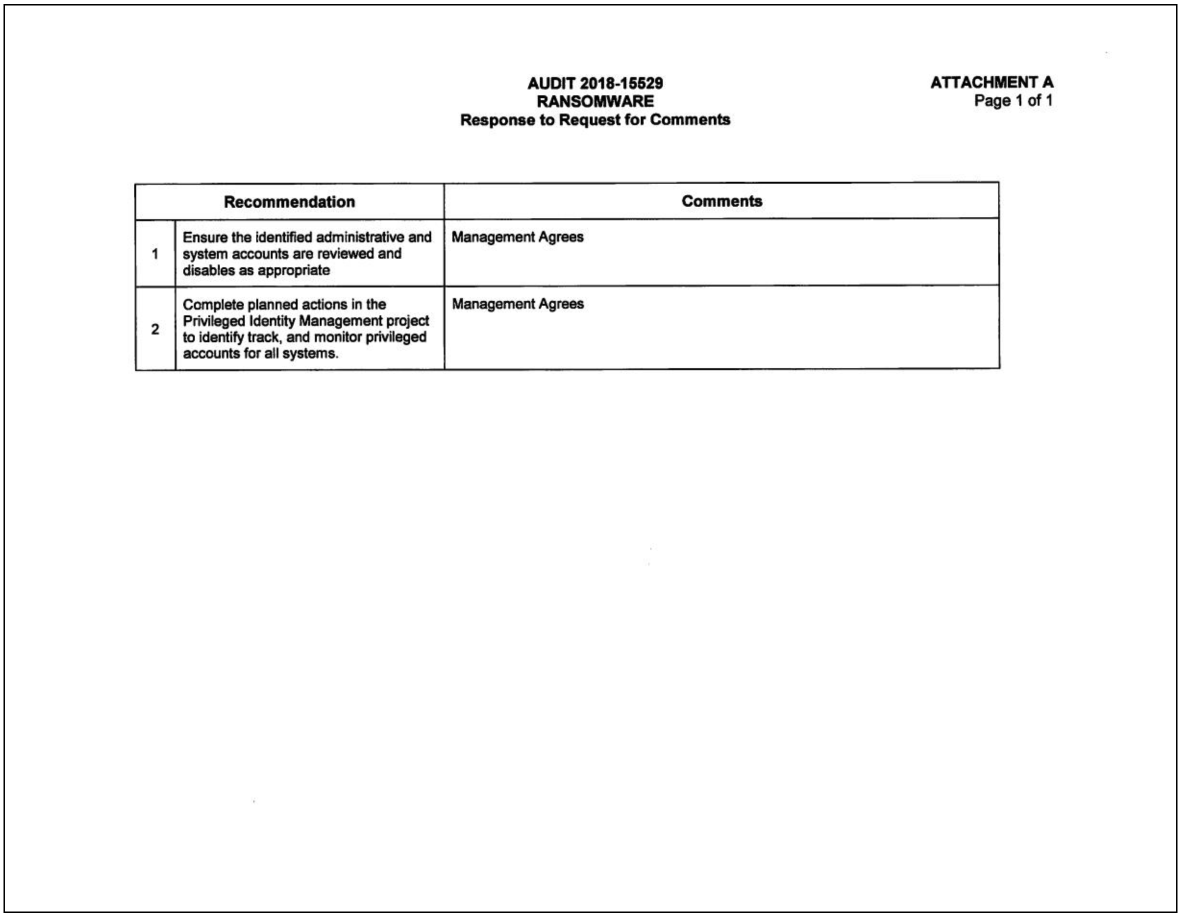
We would like to thank Sarah Huffman, Megan Spitzer, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg.

Andrea Brackett

Andrea Brackett
Director, TVA Cybersecurity
Information Technology
WT 5D-K

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

ASB:SLW
cc (Attachment):
Robert Arnold, MP 2C-C
James Berrong, SP 3L-C
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
Jeremy Fisher, MP 3B-C
Dwain Lanier, MR 6D-C
Jill Matthews, ET 4C-K
Todd McCarter, MP 2C-C
Philip Propes, SP 2A-C
Sherry Quirk, WT 7C-K
John Thomas III, MR 6D-C
OIG File No. 2018-15529



ATTACHMENT A
Page 1 of 1

AUDIT 2018-15529
RANSOMWARE
Response to Request for Comments

Recommendation		Comments
1	Ensure the identified administrative and system accounts are reviewed and disables as appropriate	Management Agrees
2	Complete planned actions in the Privileged Identity Management project to identify track, and monitor privileged accounts for all systems.	Management Agrees