Memorandum from the Office of the Inspector General

April 21, 2020

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2020-15693 – BACKUP VERIFICATION OF MISSION ESSENTIAL DATA

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority's (TVA) backup verification of mission essential data. Our objective was to determine if TVA's backups of mission essential data were being performed in accordance with business requirements and industry best practice.

In summary, we determined that TVA's backups of mission essential data included industry best practice in their business requirements. However, we found three business requirements were not being met. Specifically, we found (1) TVA was not using the enterprise authentication solution[1] as required by their common control catalog, (2) test restores were not performed for essential backup and infrastructure components, and (3) backup data in transit[2] was not encrypted.

Prior to completion of our audit, TVA management took actions to address and remediate the authentication usage finding. In addition, TVA is in the process of implementing an information technology (IT) infrastructure project that includes the latest enterprise backup solution version that will enable data in transit to be encrypted.

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

1. Determine essential backup and infrastructure components and ensure test restores of those are performed.

2. Complete the IT infrastructure project to ensure backup data is encrypted in transit.

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

[1] Management of access is centralized and monitored for all systems.

[2] Data in transit is data that is currently traveling across a network or sitting in a computer's random access memory ready to be read, updated, or processed.

BACKGROUND

Media backup and testing is a critical security control and an important part of information management practices. Ensuring the integrity and validity of backups requires proper controls and practices around the performance, protection, and restoration of data. The risks of not covering these areas range from loss of data and/or compromise of sensitive/confidential data through threats such as malware, ransomware, and/or insider threat as defined in Table 1. This can have long lasting consequences to an organization's finances, credibility, and reputation.

Threat	Definition
Malware	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Ransomware	Form of malware that targets critical data and systems for the purpose of extortion by locking the user out of the data or system. After the user is locked out of the data or system, the attacker demands a ransom payment.
Insider Threat	A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organizations security practices, data, and computer systems.

Table 1

TVA IT is responsible for performing backups and test restores of the systems it supports as defined by agreements with the TVA business units and documented internal controls. IT monitors an enterprise backup solution to ensure jobs are successful and to resolve any failed jobs.

As part of our annual audit planning, we completed a threat assessment to identify high-risk cybersecurity threats that could impact TVA. The potential for loss of data was one of those high-risk areas. In addition, TVA identified loss of data as a high impact risk in the fiscal year 2020 through 2022 IT business plan. Based on our assessment and information from TVA, we included an audit of TVA's backup verification of mission essential data as part of our 2020 audit plan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA's backups of mission essential data were being performed in accordance with business requirements and industry best practice. The scope of this audit was limited to backups of a sample of mission essential system production servers. Fieldwork was performed between November 2019 and February 2020. To meet our objective we:

- Obtained and reviewed TVA IT Standard Programs and Processes (SPP) and Work Instructions (WI), including:
  - IT-SPP-12.12.019, *Manage Data*.
  - IT-SPP-35.420, *IT Business Continuity Plan*.

  - IT-WI-12.12.010, *DBA Backup Recovery Strategy*.
  - IT-WI-12.12.023, *Media Recovery Tests – For SOX and Critical Applications*.
  - IT-WI-12.101, *Business Impact Analysis Instructions*.
- Identified applicable backup best practices from Information Systems Audit and Control Association.[3]
- Obtained and reviewed TVA's *IT Infrastructure System – Common Control Catalog* to identify business requirements.
- Judgmentally selected four systems from a population of TVA mission critical systems based on financial significance and essentialness to the backup infrastructure. For each system, we reviewed TVA's backup practices and compared them against business requirements and industry best practices.
- Conducted a walkthrough of the enterprise backup solution to obtain an understanding of the internal control environment for mission essential backups.
- Reviewed the business impact assessments to identify the recovery point objective[4] of the four judgmentally selected systems and compared to respective backup schedules and jobs.
- Assessed the design and implementation of the account management common control against the backup infrastructure.
- Inquired of TVA personnel to obtain information and understanding on TVA's backup processes and procedures.

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 determined that TVA's backups of mission essential data included industry best practice within their business requirements. However, we found three business requirements were not being met. Specifically, (1) TVA was not using the enterprise authentication solution as required by their common control catalog, (2) test restores were not performed for essential backup and infrastructure components, and (3) backup data in transit was not encrypted.

[3] Information Systems Audit and Control Association is an international professional association focused on IT governance.

[4] Recovery point objective is defined by TVA as the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of data) after an outage; the amount of data loss an organization can withstand.

AUTHENTICATION USAGE

We performed a walkthrough of the enterprise backup solution and the related storage on its data domains to obtain an understanding of the internal control environment for mission essential data backups. We found that the enterprise authentication solution was not being used to manage access to the data domains. TVA's *IT Infrastructure System – Common Control Catalog* requires an enterprise authentication system to be used for authorization of access, which allows appropriate access control and monitoring. When this is not used, there is a greater risk for insider threat due to limited access management and monitoring capabilities.

Prior to completion of our audit, TVA management informed us the data domains had been configured to utilize TVA's enterprise authentication system. We reviewed the provided documentation and confirmed the data domains had been configured appropriately.

TEST RESTORES NOT PERFORMED

Test restores are used to verify that backups are complete and accurate and could be used to restore system data if needed. TVA's *IT Infrastructure System – Common Control Catalog* states that backups are to be tested for information system configuration settings and data. Additionally, test restores are to be conducted upon initial setup of the backup routine and at least annually thereafter. We reviewed test restore documentation for four sample systems to ensure tests were successfully performed. Due to their financial significance to TVA, three of the four systems were subject to regular media recovery tests for Sarbanes Oxley (SOX) and critical applications. We found no test restores had been performed for the fourth system. Although this system was not a SOX application, it was an essential piece of TVA's backup infrastructure. Failure to perform test restores increases the risk of backup data not working if/when needed. The inability to restore an essential backup infrastructure component may prevent TVA from meeting recovery point objectives of other systems.

UNENCRYPTED DATA IN TRANSIT

TVA's *IT Infrastructure System – Common Control Catalog* states backup data should be encrypted at rest[5] and in transit. We reviewed configuration settings for the enterprise backup solution and verified data is encrypted at rest. According to TVA personnel, backup data was not encrypted in transit. To reduce the risk of data compromise and/or the exposure of confidential and/or sensitive information, TVA management relies on network segmentation that limits access to the data in transit. TVA is in the process of implementing an IT infrastructure project that includes the latest enterprise backup solution version that will enable data in transit to be encrypted.

[5] Data at rest is a term that refers to data stored on a device or backup medium such as a hard drive, backup tape, or mobile device.

RECOMMENDATIONS

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

1. Determine essential backup and infrastructure components and ensure test restores of those are performed.

2. Complete the IT infrastructure project to ensure backup data is encrypted in transit.

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.

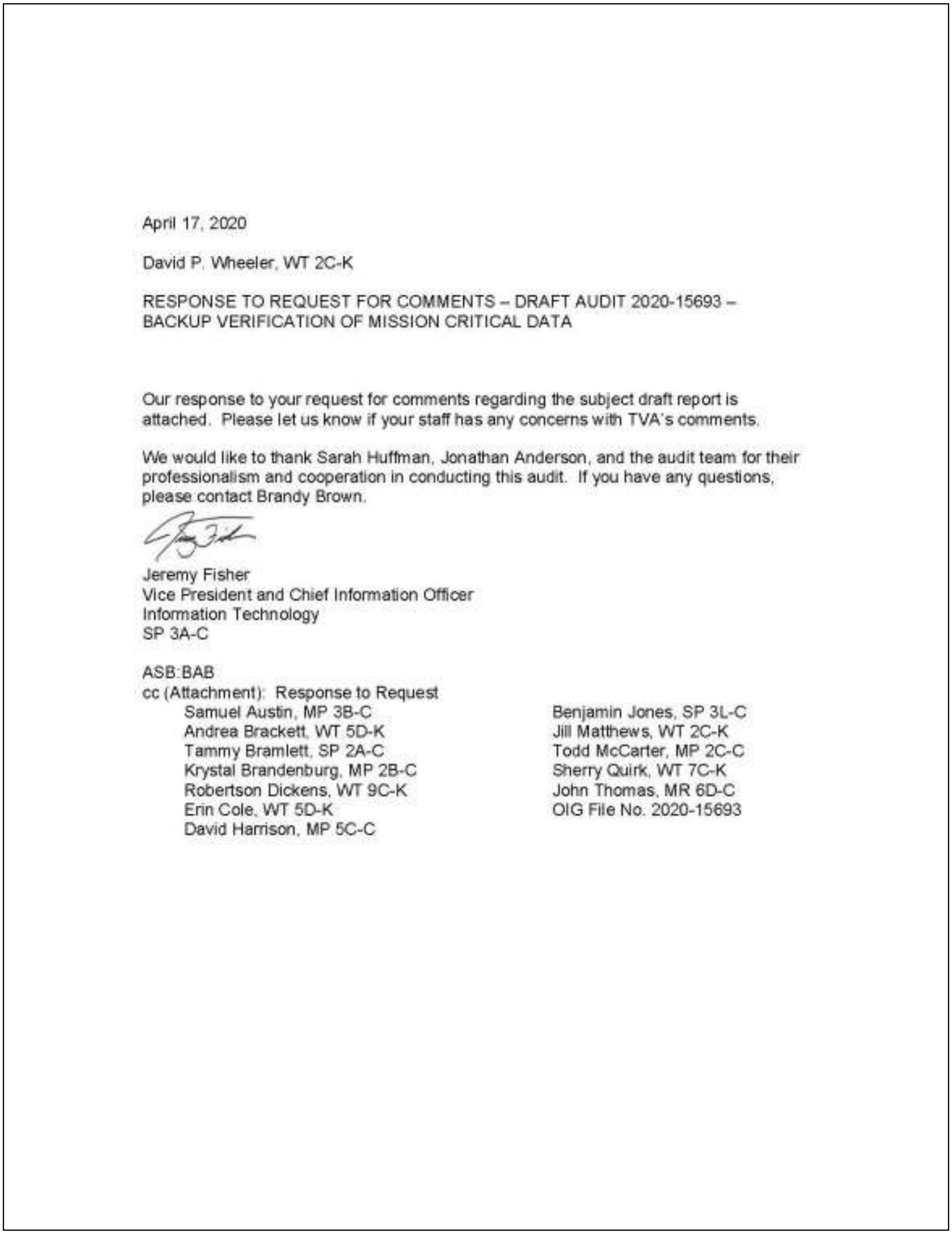
- - - - - -

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. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance. If you have any questions, please contact Jonathan B. Anderson, Senior Auditor, at (865) 633-7340 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)

JBA:KDS
cc: TVA Board of Directors
Andrea S. Brackett
Erin L. Cole
David M. Harrison
Jeffrey J. Lyash
Justin C. Maierhofer
Jill M. Matthews
Todd E. McCarter
Sherry A. Quirk
John M. Thomas III
OIG File No. 2020-15693



April 17, 2020

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2020-15693 – BACKUP VERIFICATION OF MISSION CRITICAL DATA

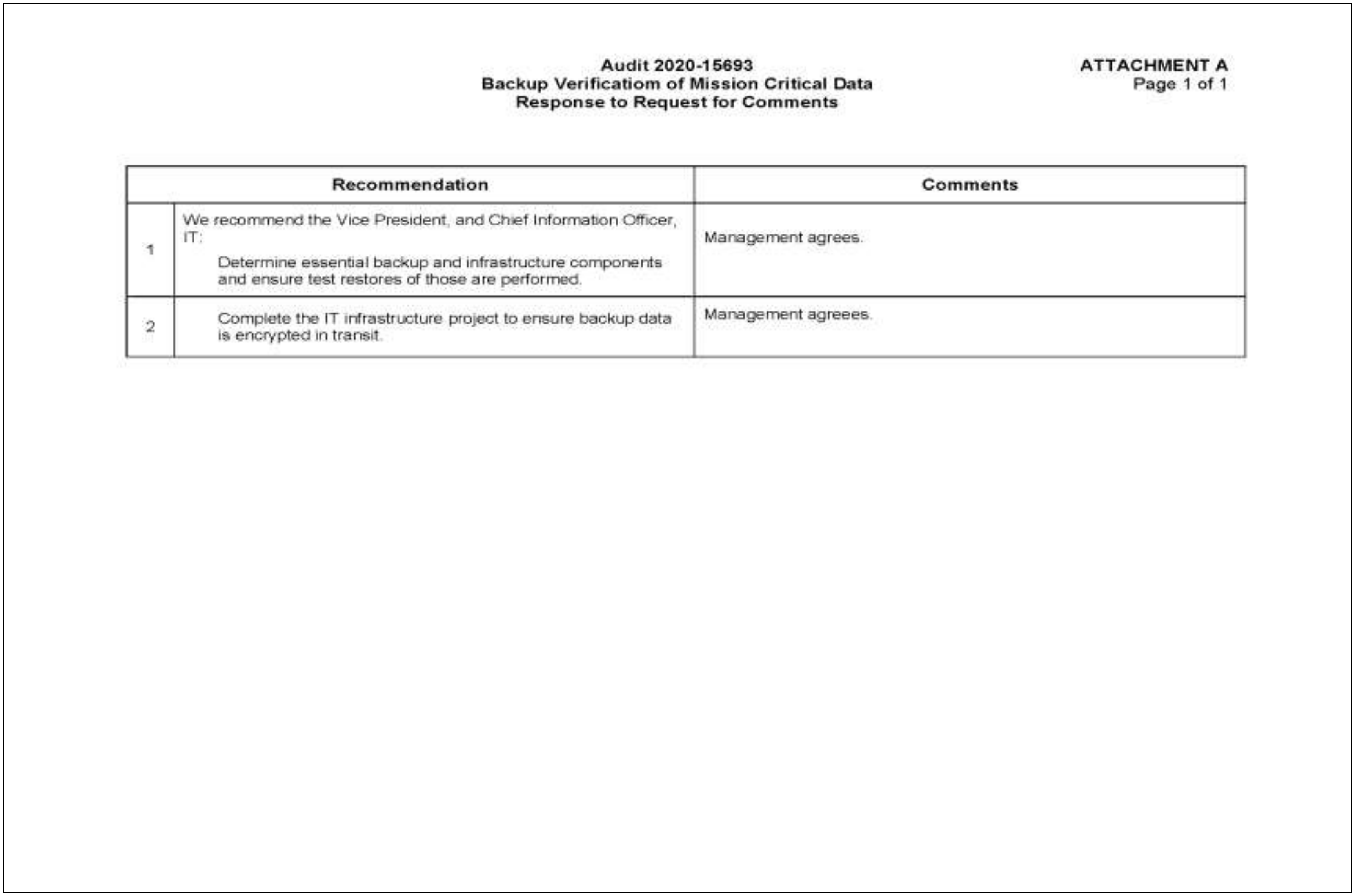
Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Jonathan Anderson, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brandy Brown.

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

ASB:BAB
cc (Attachment): Response to Request
Samuel Austin, MP 3B-C
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
Erin Cole, WT 5D-K
David Harrison, MP 5C-C
Benjamin Jones, SP 3L-C
Jill Matthews, WT 2C-K
Todd McCarter, MP 2C-C
Sherry Quirk, WT 7C-K
John Thomas, MR 6D-C
OIG File No. 2020-15693

APPENDIX
PAGE 2 OF 2



ATTACHMENT A
Page 1 of 1

Audit 2020-15693
Backup Verificatiom of Mission Critical Data
Response to Request for Comments

Recommendation		Comments
1	We recommend the Vice President, and Chief Information Officer, IT: Determine essential backup and infrastructure components and ensure test restores of those are performed.	Management agrees.
2	Complete the IT infrastructure project to ensure backup data is encrypted in transit.	Management agreees.