Memorandum from the Office of the Inspector General

February 26, 2026

Kris G. Edmondson
Michelle R. Ray

REQUEST FOR MANAGEMENT DECISION – AUDIT 2025-17557 – BACKUP AND RECOVERY OF OPERATIONAL TECHNOLOGY – GAS OPERATIONS

Due to the risk of critical equipment failure, cyber exploitation of generation assets, and a previous audit finding related to contingency plans at gas plants,[1] we performed an audit of backup and recovery of operational technology (OT) assets at Tennessee Valley Authority's (TVA's) natural gas plants. Our objectives were to determine if the backup and recovery process for operational technology cyber assets at TVA natural gas plants were (1) designed in accordance with federal guidance and (2) operating as defined by TVA policy.

We determined TVA Generation's backup and recovery procedure was designed in accordance with federal guidance for most areas. However, the (1) procedure did not align with federal guidance for encryption and (2) process was not operating as defined by TVA Generation's procedure. Specifically, National Institute of Standards and Technology (NIST)[2] recommends cryptographic mechanisms[3] be implemented to prevent unauthorized disclosure and modification of data; however, encryption was not addressed in Generation's procedure. Additionally, none of the plants selected for testing had a documented backup and recovery plan as required by procedure.

We recommend the Vice President, Generation Tech Support, (1) revise and communicate the backup and recovery procedure and (2) develop backup and recovery plans for each plant. In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

BACKGROUND

Within the TVA natural gas fleet, there are nine combustion turbine and eight combined cycle plants that can produce over 12,000 megawatts of electricity – enough to power

---

1 Audit Report 2023-17433, *Operational Technology Cybersecurity – Combined Cycle Plant*, June 17, 2024.

2 NIST Special Publication 800-53 (Revision 5), Security and Privacy Controls for Information Systems and Organizations, September 2020, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>, accessed on September 8, 2025.

3 Cryptographic mechanisms refers to types of encryption.

about 7 million homes, as of December 2025. As part of the greater interconnected power grid, natural gas plants are a vital element in the power mix.

Protecting against cybersecurity threats and equipment failures is vital to the organization's mission and business functions. Power plants rely on OT to ensure the plants can run without disruption. OT systems and devices monitor or control physical processes or events and encompass a large range of assets from servers to computers. Implementing backup and recovery controls can reduce the risk of cyber attacks to OT assets and ensure availability and integrity of information systems. TVA documents these controls in a Generation Standard Operating Procedure (SOP).

In the previous audit, we determined logical, physical, and general security controls were designed and operating effectively at one combined cycle plant; however, contingency plans were not documented. We recommended the site develop a contingency plan. As a result of the finding, TVA Generation updated the SOP that focuses on the backup and recovery process.

Due to the risk of critical equipment failure, cyber exploitation of generation assets, and a previous audit finding related to contingency plans at gas plants, we audited TVA's backup and recovery process for OT cyber assets at TVA natural gas plants for alignment with federal guidance and compliance with a TVA Generation SOP.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objectives were to determine if the backup and recovery process for operational technology cyber assets at TVA natural gas plants were (1) designed in accordance with federal guidance and (2) operating as defined by TVA policy. Our scope was limited to the OT cyber assets at TVA natural gas plants. To achieve our objective, we:

- Conducted interviews and walkthroughs with TVA Generation personnel to understand the backup and recovery process.
- Reviewed TVA Generation SOP 12.871, *Cyber Security – Backup and Recovery*, to understand backup and recovery procedure requirements at TVA natural gas plants.
- Selected 4 of 17 natural gas plants for SOP compliance testing. Our selection was made judgmentally based on a prior audit finding and varying megawatt output across the Tennessee Valley.
- Reviewed internal controls to the extent necessary to address the audit objective, including:
  - Identified backup and recovery controls as significant information system controls.
  - Assessed design of internal controls by comparing the backup and recovery process to federal guidance from NIST.
  - Assessed implementation and operating effectiveness of backup and recovery controls by reviewing the selected natural gas plants' processes and documentation to determine alignment with procedure requirements.

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 TVA Generation SOP 12.871, *Cyber Security – Backup and Recovery,* was designed in accordance with federal guidance for the following areas: backups, restoration testing, reliability and integrity testing, critical and alternate storage, recovery, and restoration within timeframe. However, we determined (1) the SOP did not align with federal guidance for encryption, and (2) the backup and recovery process was not operating as defined by the SOP at any of the selected plants. Specifically, encryption was not addressed in the procedure, and none of the plants selected for testing had a documented backup and recovery plan as required.

BACKUP AND RECOVERY PROCEDURE DID NOT ALIGN WITH FEDERAL GUIDANCE FOR ENCRYPTION

The SOP addressed three moderate and four high security baseline backup and recovery controls from NIST with one additional moderate baseline control not applicable to TVA's systems. However, we identified the moderate baseline requirement for encryption was not addressed in TVA's SOP. NIST recommends cryptographic mechanisms be implemented to prevent unauthorized disclosure and modification of data. If backup data is unencrypted, it risks the confidentiality and integrity of the backups.

BACKUP AND RECOVERY PROCESS IS NOT OPERATING AS DEFINED BY PROCEDURE

We determined the backup and recovery process at the plants was not implemented or operating as defined by the procedure. The SOP requires each plant to create and implement a backup and recovery plan with specific elements. However, a documented plan was not in place at the four plants we reviewed. In addition, responsible individuals we interviewed at the plants were unaware of the procedure requirements. All four plants performed periodic backups, and personnel at one plant indicated they had conducted a recovery; however, without a documented backup and recovery plan, a plant could be unprepared for a scenario requiring recovery, such as ransomware or equipment failure.

RECOMMENDATIONS

We recommend the Vice President, Generation Tech Support:

1. Revise TVA Generation's SOP 12.871, *Cyber Security – Backup and Recovery,* to address encryption to align with federal guidance and communicate the SOP requirements to plant personnel.

2. Develop backup and recovery plans for each plant in accordance with TVA Generation's SOP 12.871, *Cyber Security – Backup and Recovery*.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendations. 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. 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 Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

Greg Stinson
Assistant Inspector General
(Audits and Evaluations)

MES:KDS
cc: TVA Board of Directors
Allen A. Clare
Jessica Dufner
T. Daniel Lunsford
Jill M. Matthews
Edward C. Meade
Donald A. Moul
Jason T. Regg
Ronald R. Sanders II
Bevin W. Taylor
Ben R. Wagner
OIG File No. 2025-17557

February 18, 2026

Greg Stinson, WT 2C-K

REQUEST FOR COMMENTS – DRAFT AUDIT 2025-17557 – BACKUP AND RECOVERY OF OPERATIONAL TECHNOLOGY - GAS OPERATIONS

Gas Operations would like to thank Megan Spitzer and Sarah E. Huffman for their diligence and support in identifying opportunities for the backup and recovery of operational technology in Gas Operations.

This is in response to your memorandum dated February 04, 2026. After reviewing the draft evaluation, please see the following responses.

Recommendations
We recommend the Vice President, Generation Tech Support:

1. Revise TVA Generation's SOP 12.871, *Cyber Security - Backup and Recovery*, to address encryption to align with federal guidance and communicate the SOP requirements to plant personnel.

   Response
   Generation Tech Support and Gas Operations agree with the recommendation.

2. Develop backup and recovery plans for each plant in accordance with TVA Generation's SOP 12.871, *Cyber Security - Backup and Recovery*.

   Response
   Generation Tech Support and Gas Operations agree with the recommendation.

Thank you for allowing us the time to review and provide feedback on the draft audit.

Kris Edmondson
Vice President
Gas Operations

Michelle Ray
Vice President
Generation Tech Support

TDL
cc:
Allen A. Clare
T. Daniel Lunsford
Edward C. Meade
Jason T. Regg
Ronald R. Sanders II
OIG File No. 2025-17557