Memorandum from the Office of the Inspector General

September 24, 2026

Joshua Linville

REQUEST FOR MANAGEMENT DECISION – AUDIT 2025-17556 – LOST OR STOLEN INFORMATION TECHNOLOGY ASSETS

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. 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 or wish to discuss our findings, 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)

FBL:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Kaitlyn R. Bennett
Kenneth C. Carnes II
Hannah S. Clements
Sherri R. Collins
Jessica E. Dufner
Jill M. Matthews
Todd E. McCarter
Edward C. Meade
Ronald R. Sanders II
Michael D. Skaggs
Bevin W. Taylor
William M. Trumm
Michael S. Turnbow
Ben R. Wagner
OIG File No. 2025-17556

Office of the Inspector General

Audit Report

To the Senior Vice President,
Chief Information Officer,
Information Technology

LOST OR STOLEN INFORMATION TECHNOLOGY ASSETS

Audit Team
Frank B. Lord
Megan E. Spitzer

Audit 2025-17556
September 24, 2026

ABBREVIATIONS

CISA	Cybersecurity and Infrastructure Security Agency
FISMA	Federal Information Security Modernization Act of 2014
IAP	Incident Action Plan
IT	Information Technology
PII	Personally Identifiable Information
SPP	Standard Programs and Processes
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

BACKGROUND 1

OBJECTIVE, SCOPE, AND METHODOLOGY 2

FINDINGS 3

TVA DID NOT FULLY COMPLY WITH FEDERAL REPORTING REQUIREMENTS 3

TVA DID NOT ALWAYS FOLLOW POLICIES AND PROCEDURES 3

ADDITIONAL INFORMATION 5

RECOMMENDATIONS 6

APPENDIX

MEMORANDUM DATED SEPTEMBER 18, 2026, FROM JOSHUA LINVILLE TO GREG STINSON

Audit 2025-17556 – Lost or Stolen Information Technology Assets

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Tennessee Valley Authority (TVA) manages devices that may contain critical infrastructure information, personally identifiable information, or sensitive business information. Failure to properly handle and report lost or stolen devices[i] increases the risk of unauthorized access to TVA data. TVA has processes and controls designed to address the risks associated with lost or stolen devices; including:

- Incident action plans – Plans that serve as a basis for the response to an incident and informs TVA personnel on steps to take in response.
- Asset verification – A process used by TVA to identify devices that have not been active for over 60 days.
- Remote management capabilities – Tools used to monitor and remotely wipe devices with sensitive business information.
- Device encryption – Tool used to protect sensitive information from unauthorized information disclosure in the event a device is lost or stolen.

Additionally, the *Federal Information Security Modernization Act of 2014* requires federal agencies to report incidents to the Cybersecurity and Infrastructure Security Agency (CISA). CISA's *Federal Incident Notification Guidelines* require loss or theft of a computing device or media used by the organization to be reported as incidents.

Due to the risks associated with lost or stolen devices, we conducted an audit to determine if TVA follows policies, procedures, and federal guidance for lost or stolen devices. The scope of our audit included devices managed by TVA's Information Technology (IT) organization that were categorized as lost or stolen within TVA's asset management system as of July 10, 2025. As of that date, TVA IT managed 23,518 computers and 9,017 handheld devices in the IT asset management system. Of these devices, a total of 267 (236 computers and 31 handheld devices) were categorized as lost or stolen.

[i] Devices include computers (i.e., laptops and desktops) and handheld devices (i.e., tablets and mobile phones).

Audit 2025-17556 – Lost or Stolen Information Technology Assets

EXECUTIVE SUMMARY

What the OIG Found

We determined TVA did not comply with federal requirements because at least 127 of 267 lost or stolen devices were not reported to CISA. We were unable to determine if an additional 98 devices were reported due to incomplete records. We also determined TVA did not follow policies and procedures related to lost or stolen IT assets. Specifically, TVA did not complete an incident action plan for most lost or stolen devices and did not always complete the asset verification process in a timely manner. Additionally, we found controls TVA had in place to address the risk of unauthorized information disclosure from lost or stolen devices were not implemented consistently, including (1) remote-wipe capabilities and (2) encryption.

In addition, we determined that TVA controls related to lost or stolen devices were appropriately designed in accordance with federal guidelines. However, based on the policies and procedures not being consistently followed, we determined they were not effectively implemented.

What the OIG Recommends

We made five recommendations to TVA management to report lost or stolen devices in accordance with federal reporting guidelines, increase adherence to internal policies and procedures for handling lost or stolen devices, and enforce controls for remote management capabilities and device encryption where technically feasible.[ii]

TVA Management's Comments

In response to our draft audit report, TVA management agreed with each of the recommendations in the report. See the Appendix for TVA management's complete response.

[ii] Prior to receiving TVA's response to our draft audit report, we had discussions with TVA management regarding clarification of three recommendations that we revised accordingly.

BACKGROUND

The Tennessee Valley Authority (TVA) Information Technology (IT) organization manages devices that may contain critical infrastructure information, personally identifiable information (PII), or sensitive business information. Failure to properly handle and report lost or stolen devices[1] increases the risk of unauthorized access to TVA data. TVA has established the following Standard Programs and Processes (SPPs) to address lost or stolen devices.

- TVA-SPP-12.405, *IT Asset Procurement & Management*, details the asset verification process. The process requires an investigation to determine if a device should be categorized as lost or stolen when it has not been active or connected to the TVA network for 60 days.
- TVA-SPP-12.006, *Cyber Incident Response,* requires an incident action plan (IAP) to be initiated when a device is identified as missing. The IAP includes steps to (1) determine if the device contained PII or sensitive business information, (2) conduct a remote wipe of the asset if it contains PII or sensitive business information, (3) update the asset status as lost or stolen in TVA's remote management tool, (4) submit a report to Cybersecurity and Infrastructure Security Agency (CISA), and (5) update the incident ticket to document steps taken.
- TVA-SPP-12.002, *Information Management Policy,* requires full disk encryption on electronically stored information, to protect against unauthorized information disclosure. According to TVA personnel, TVA has (1) required full-device encryption since 2018 on newly deployed laptops and (2) deployed tablets and mobile phones that manage full-disk encryption through mobile device management.

The *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies to develop procedures for detecting, responding to, and reporting security incidents to CISA. CISA's Federal Incident Notification Guidelines require reporting incidents such as loss or theft of equipment, phishing, web attacks, etc. The guidelines state cyber incidents must be reported to CISA within an hour of being identified by the agency. CISA collects cyber incident reports from federal agencies to help safeguard the nation's critical infrastructure.

TVA-SPP-12.002 and TVA-SPP-12.006 include requirements to comply with FISMA. TVA-SPP-12.002 requires users to report lost or stolen IT devices to TVA's IT organization. TVA-SPP-12.006 requires TVA's lost or stolen devices to be reported to CISA within an hour of incident confirmation.

As of July 10, 2025, TVA's IT asset management system showed a population of 23,518 active computers, consisting of laptops and desktops, and 9,017 active handheld devices, consisting of tablets and mobile phones. At that time, a total

[1] Devices include computers (i.e., laptops and desktops) and handheld devices (i.e., tablets and mobile phones).

of 267 were categorized as lost or stolen, including 236 computers and 31 handheld devices.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA follows policies, procedures, and federal guidance for lost or stolen devices. Our scope included TVA IT-managed computers and handheld devices categorized as lost or stolen within TVA's asset management system, as of July 10, 2025. To achieve our objective, we:

- Conducted interviews with TVA personnel to understand the process for identifying, categorizing, and reporting lost or stolen devices.
- Reviewed relevant federal laws and guidance to gain an understanding of federal requirements for reporting lost or stolen devices:
  - FISMA
  - CISA's *Federal Incident Notification Guidelines*
- Reviewed TVA agency-wide policies and procedures to gain an understanding of how TVA handles lost or stolen devices:
  - TVA-SPP-12.002, *TVA Information Management Policy*
  - TVA-SPP-12.006, *Cyber Incident Response*
  - TVA-SPP-12.405, *IT Asset Procurement & Management*
- Obtained the total population of lost or stolen devices as of July 10, 2025, from TVA's IT asset management system to assess TVA's incident response process.
- Reviewed internal controls to the extent necessary to address the audit objective, including:
  - Identified (1) cybersecurity incident reporting controls and (2) hardware asset management verification controls as significant to our audit objective.
  - Assessed design of internal controls by comparing TVA's process for reporting lost or stolen devices to federal law and guidelines.
  - Assessed implementation of internal controls by reviewing lost or stolen IT asset records, associated incident action plans, and corresponding CISA reports.

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 did not comply with federal requirements because at least 127 of 267 lost or stolen devices were not reported to CISA. We were unable to determine if 98 devices were reported due to incomplete records. We also determined TVA did not follow policies and procedures related to lost or stolen IT assets. Specifically, TVA did not complete an IAP for most lost or stolen devices and did not always complete the asset verification process in a timely manner. Additionally, we found that controls TVA had in place to address the risk of unauthorized information disclosure from lost or stolen devices were not implemented consistently, including (1) remote-wipe capabilities and (2) encryption.

In addition, we determined that TVA controls related to lost or stolen devices were appropriately designed in accordance with federal guidelines. However, based on the policies and procedures not being consistently followed, we determined they were not effectively implemented.

TVA DID NOT FULLY COMPLY WITH FEDERAL REPORTING REQUIREMENTS

TVA had a population of 267 lost or stolen devices as of July 10, 2025, consisting of 236 computers and 31 handheld devices. FISMA requires federal agencies to report cyber incidents to CISA within an hour of incident declaration, including instances of lost or stolen devices. We compared TVA's incident records in the IT asset management system to incident reports submitted to CISA for the 267 lost or stolen devices. We determined 42 lost or stolen devices were reported to CISA, and 127 devices were not reported. We were unable to determine if the remaining 98 devices had been reported due to incomplete records. When incidents are not reported to CISA in a timely manner, CISA is prevented from timely identification of systemic vulnerabilities or sharing intelligence to protect the nation's critical infrastructure.

TVA DID NOT ALWAYS FOLLOW POLICIES AND PROCEDURES

We reviewed asset management records associated with the 267 lost or stolen devices and determined that TVA policies and procedures were not always followed. Specifically, TVA did not complete an IAP for most lost or stolen devices and did not always complete the asset verification process in a timely manner.

TVA Did Not Complete an Incident Action Plan for Most Lost or Stolen Devices

When a TVA device is identified as lost or stolen, an IAP should be initiated and completed in accordance with TVA-SPP-12.006, *Cyber Incident Response*. The IAP steps include (1) determining if the asset contained PII or sensitive business information, (2) conducting a remote wipe of the asset if the asset contains PII or

sensitive business information, (3) updating the asset status as lost or stolen in TVA's remote management tool, (4) submitting a report to CISA, and (5) updating the incident ticket to document steps taken.

We reviewed tickets associated with the 267 lost or stolen devices and found TVA did not complete an IAP for most of its lost or stolen devices. Specifically, we determined only 3 of the 267 lost or stolen devices had documentation to support an IAP had been fully completed. For the remaining 264, at least one of the five IAP required steps were not completed as shown in Table 1.[2]

IAP Required Steps	Devices Completed
1. PII assessed	28
2. Remote wipe	35
3. Update status as lost or stolen	267
4. Reported to CISA	42
5. Update incident Ticket	3

Table 1

Without completing and documenting each step of the IAP, TVA cannot consistently mitigate the risks associated with unauthorized information disclosure.

TVA Did Not Always Complete the Asset Verification Process in a Timely Manner

TVA-SPP-12.405, *IT Asset Procurement & Management,* states the asset verification process is intended to check the accuracy of the asset management system. The SPP requires an investigation be performed to locate or retire a device after 60 days of a device's inactivity or not connecting to the TVA network. TVA's asset management system generates an investigation task to be addressed by IT after 60 days of inactivity.

Asset investigation tasks were created for 74 lost or stolen devices in the asset management system. TVA-SPP-12.405 does not define a timeframe for completing these investigations. However, as shown in Table 2, 59 of the 74 investigation tasks took over 6 months to complete, which we determined to be untimely.

[2] During the audit, TVA provided documentation from a separate automated process that showed some required IAP steps were completed that were not documented in TVA's asset management system, we included those actions in Table 1.

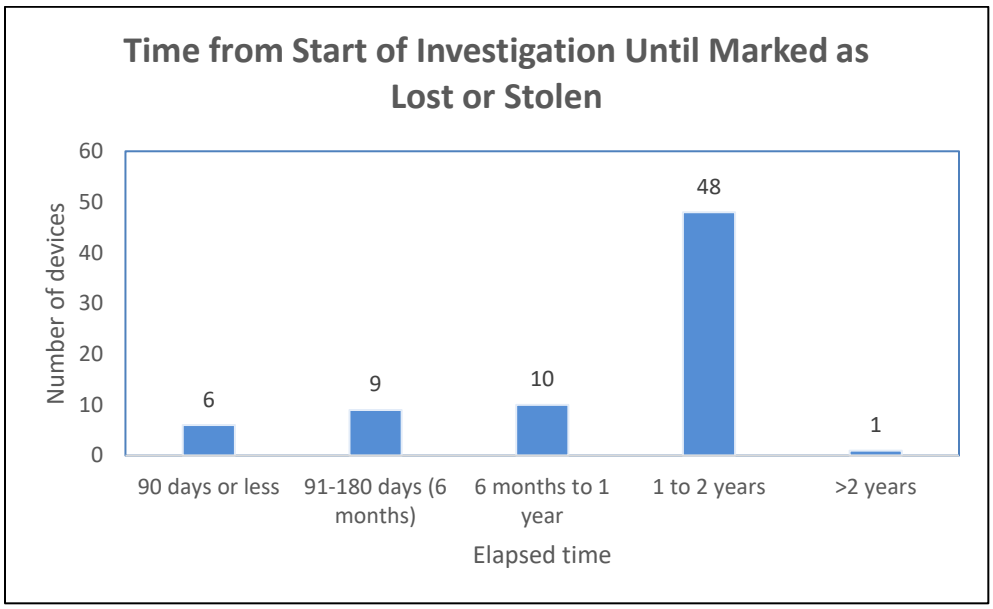


Table 2

Without timely identification of a lost or stolen device, appropriate incident response procedures cannot be performed.

ADDITIONAL INFORMATION

We reviewed controls TVA had in place to address the risk of unauthorized information disclosure from lost or stolen devices. We determined TVA did not fully implement remote-wipe capabilities or consistently enforce encryption on its devices.

TVA Did Not Fully Implement Remote-Wipe Capabilities

As stated previously, TVA's IAP requires any lost or stolen devices that contain PII or sensitive business information be remotely wiped. We found 203 of 236 computers did not have remote-wipe tools installed, which would prevent TVA from performing remote wipe if necessary. Specifically, 128 of the 203 computers were laptops, which pose a higher risk of loss or theft due to ease of mobility over desktops. Failure to fully implement remote wiping across laptops could result in increased risk of unauthorized information disclosure and reputational damage.

TVA Did Not Consistently Enforce Encryption

TVA-SPP-12.002, *Information Management Policy,* requires device data to be encrypted to protect TVA from unauthorized information disclosure in the event a device is lost or stolen. We reviewed device encryption on 31 handheld devices and 166[3] computers and determined that all 31 handheld devices were encrypted; however, 71 of the 166 computers were not encrypted. Therefore, device encryption was not consistently enforced across the lost or stolen computers.

[3] Of the 236 computers, 166 were deployed after the 2018 encryption requirement was implemented.

RECOMMENDATIONS

We recommend the Senior Vice President and Chief Information Officer:[4]

1. Take steps to comply with CISA reporting requirements for all lost or stolen devices.

2. Review the IAP process and implement controls to ensure required steps are completed and documented.

3. Review and update the asset verification process to establish a timeframe for timely completion.

4. Consistently implement remote-wipe capabilities for IT-managed laptops where technically feasible.

5. Enforce device encryption requirements for IT-managed laptops and desktops where technically feasible.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with each of our recommendations. See the Appendix for TVA management's complete response.

[4] Prior to receiving TVA's response to our draft audit report, we had discussions with TVA management regarding clarification of Recommendations 3, 4, and 5 and revised the recommendations accordingly.

September 18, 2026

Greg Stinson, WT 2C

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2025-17556 – LOST OR STOLEN INFORMATION TECHNOLOGY ASSETS

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, Frank B. Lord, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Dustin Pate.

Joshua Linville
Senior Vice President & Chief Information Officer
Information Technology

KCC: BAA
cc (Attachment): Response to Request

Kaitlyn R. Bennett
Lindsay N. Bramlett
Lara M. Butler
Kenneth C. Carnes II
Hannah S. Clements
Sherri R. Collins
Andrew Craig
Melissa R. Crane
Mark A. Howard
Gregory G. Jackson
Melissa A. Livesey
Todd E. McCarter
Edward C. Meade
Dustin C. Pate
Ronald R. Sanders II
Francisco J. Soutuyo
Courtney L. Stetzler
Paul B. Trachian
Michael S. Turnbow
William M. Trumm
OIG File No. 2025-17556

Audit 2025-17556 – Lost or Stolen Information Technology Assets

ATTACHMENT A
Page 1 of 1

Response to Request for Comments

	Recommendation	Comments
1	We recommend the Senior Vice President and Chief Information Officer: Take steps to comply with CISA reporting requirements for all lost or stolen devices.	Management agrees.
2	Review the IAP process and implement controls to ensure required steps are completed and documented.	Management agrees.
3	Review and update the asset verification process to establish a timeframe for timely completion.	Management agrees.
4	Consistently implement remote-wipe capabilities for IT-managed laptops where technically feasible.	Management agrees.
5	Enforce device encryption requirements for IT-managed laptops and desktops where technically feasible.	Management agrees.