Light Rail Safety Audit Report (26-08)

Agenda Item 6. c.

Audit Scope

- Period of Review: January 1, 2025 – December 31, 2025. Other periods reviewed as necessary.
- Audit topics:
  - Authority and policy Statement
  - Overview of Management Structure
  - Hazardous Materials Program
  - Internal Safety Audit/Review Program
  - Safety Data Collection and Analysis
  - Facilities, Structures, and Equipment Inspections
  - Maintenance Audits and Inspection Program
  - TASP Implementation Activities and Responsibilities
  - Local, State, and Federal Requirements
  - Threat and Vulnerability Identification, Assessment and Resolution
  - Implementation and Evolution of the System Security Plan (SSP)
  - Modification of the SSP

Audit Results

- Internal Audit completed the audit on June 5, 2026.
- A report was issued to the UTA Director of Safety and Security
- The report was limited to observations with no recommendations
- It is the decision of the State Safety Oversight (SSO) and Safety Department what observations to address and how to address them. The Federal Transit Administration reviews the results of the audit and how findings are addressed.

Audit Results

- Findings of Compliance with Recommendations
  - IA found that a number of operations and maintenance personnel were not aware of who the Light Rail Safety Administrator is. IA recommends that the Safety Department identify ways to make the Light Rail staff aware of who the Safety Administrator is through regular contact.
  - Currently have two versions of the Transit Agency Safety Plan (TASP), one adopted in 2024 and a 2026 version awaiting approval from the JLMSC at which point it will be adopted. IA recommends that the 2026 TASP be approved by the JLMSC and adopted.
  - Safety Department find ways to make the Light Rail staff aware of where to locate hazardous material information within the UTA SharePoint website.

Audit Results Continued

- IA recommends that Safety identify ways to make the OSHA injury/illness log more readily available to all members of management, and/or create a centralized distribution list.

- The auditor noted that the System Security Plan (SSP) could be improved by adding more specific instructions on how to evaluate the severity of issues in determining whether a CAP is necessary and recommends that Security take steps to develop and include these instructions in the SSP.