BOARD OF DIRECTORS

METROPOLITAN ATLANTA RAPID TRANSIT AUTHORITY

AUDIT COMMITTEE

THURSDAY, MARCH 20, 2025

ATLANTA, GEORGIA

MEETING SUMMARY

1. CALL TO ORDER AND ROLL CALL

Committee Chair Freda Hardage called the meeting to order at 10:04 A.M.

Board Members Present:	James Durrett Roderick Frierson Freda Hardage Al Pond Kathryn Powers Rita Scott Valencia Williamson Jennifer Ide Jacob Tzegaegbe Sagirah Jones Shayna Pollock
Board Members Absent:	Russell McMurry Thomas Worthy Jannine Miller Elizabeth Bolton-Harris
Staff Members Present:	Collie Greenwood Steven Parker Jonathan Hunt LaShanda Dawkins Carrie Rocha Rhonda Allen Ralph McKinney Michael Kreher

George Wright
Kevin Hurley

Also in Attendance: Justice Leah Ward Sears, Emil Tzanov, Lawrence Williams, Paula Nash, Jacqueline Holland, Tyrene Huff, Kenya Hammond, Phyllis Bryant

2. APPROVAL OF THE MINUTES

Minutes from November 22, 2024
Approval of the Minutes from November 22, 2024, Audit Committee meeting. On a motion by Board Member Powers, seconded by Board Member Durrett, the motion passed by a vote of 7 to 0 with 7 members present.

3. BRIEFING

Internal Audit Q2 /FY25 Activity
Emil Tzanov, AGM of Internal Audit, briefed the Committee on Internal Audit activity for the Q2 of FY25.

Information Security Activity Update
Lawrence Williams, AGM of Information Security, presented an information security update.

KPMG Report
Collie Greenwood, MARTA's General Manager/CEO, provided a verbal follow-up to the KPMG assessment requested by MARTOC. Board Members discussed forming an Ad Hoc Committee on More MARTA Enhanced Bus Service Allocation.

4. OTHER MATTERS
None

5. ADJOURNMENT
The Committee meeting adjourned at 11:21 A. M.

YouTube link: https://www.youtube.com/watch?v=PBxN8xbhvYY

Internal Audit Activity Briefing

Q2 / FY25 ~ Oct 1 – Dec 31, 2024

Operational Group Audits

Q2 / FY25 A

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Capital Program - Summerhill BRT	TBD	TBD	Planning	-	-	-	-	-	-	-	-
Rail Stations Management	TBD	TBD	Planning	-	-	-	-	-	-	-	-
Clayton Co Ops & Maintenance Facility	12/20/24	High Risk	Reporting	4	-	4	-	3	-	3	-

- *Project Management Plan and FTA Quarterly Milestone Progress Reporting were not up to date. (Date: TBD)*
- *Lack of Project Management Monitoring and Oversight. (Date: TBD)*
- *Inefficient use of project schedule control tool. (Date: TBD)*
- *Inefficient use of Document and Record project control tools. (Date: TBD)*

Operational Group Audits Q2 / FY25 B

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Bus Operations – CDL & Medical Cards Mgmt.	12/3/24	High Risk	Completed	3	-	2	1	-	-	-	-
		- *Commercial Driver's License Program procedures out of date (2/15/2025)* - *Bus Operations is not in compliance with 49 CFR 383.33 (1/31/2025)* - *Bus Operations is not in compliance with 49 CFR 383.51 (3/31/2025)*									
Employee Timekeeping	10/16/24	Needs Attention	Completed	1	-	1	-	1	-	1	-
		- *Excessive manual processes / Teledriver replacement (7/15/2025)*									
Indian Creek Station	2/13/25	High Risk	Completed	3	-	3	-	2	-	2	-
		-Lack of documented Project Management Plan. (Date: TBD) *-Incomplete risk documentation and the absence Risk Management Plan. (Date: TBD)* *-Contract or work order deliverables cannot be clearly tracked. (Date: TBD)*									
Total Significant & Moderate Findings:				**11**	**-**	**10**	**1**	**6**	**-**	**6**	-

Prior Operational Audits with Open Findings

A

Audit Title	Audit Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Mobility Service	6/26/24	High Risk	Completed	3	3	-	-	-	-	-	-
Wayside Access & Safety	3/19/24	Needs Attention	Completed	1	1	-		2	1	1	-
Attracting & Retaining Employees	6/28/23	High Risk	Completed	4	4	-	-	4	4	-	-

- *Contract modifications without updated Independent Cost Estimates (ICEs) (12/1/24)*
- *Ineffective contract oversight related to various contract language clauses (12/1/24)*
- *Unauthorized commitments bypassing the contract modification process (12/1/24)*

Prior Operational Audits with Open Findings

B

Audit Title	Audit Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Review of Transit Oriented Development	5/15/23	Needs Attention	Completed	3	2	1	-	1	-	1	-
		- *The Office of Real Estate does not have an asset management System (3/31/2025).*									
Capital Projects – Soft Cost	9/30/22	Needs Attention	Completed	-	-	-	-	2	1	1	-
Capital Improvement Program Follow-up	1/15/21	Needs Attention	Completed	28	21	7	-	-	-	-	-
Total Significant & Moderate Findings:				**39**	**31**	**8**	-	**9**	**6**	**3**	-

IT Group Audits

Q2 / FY25

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Train Control/ SCADA Access Management Audit	TBD	TBD	Fieldwork	-	-	-	-	-	-	-	-
Software Maintenance	12/18/24	High Risk	Completed	3	-	3	-	-	-	-	-
Windows 10 Enterprise End Of Life Plan Review	10/21/24	High Risk	Completed	1	-	1	-	-	-	-	-
Total Significant & Moderate Findings:				**4**	**-**	**4**	**-**	**-**	**-**	**-**	**-**

Prior IT Audits with Open Findings

Audit Title	Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
IT Software Asset Management	7/29/24	High Risk	Completed	4	-	1	3	-	-	-	-
Elements of IT Operations	04/12/24	High Risk	Completed	5	-	-	5	2	-	-	2
IT Support of Critical Enterprise Applica-tions and Systems	11/08/23	High Risk	Completed	1	1	-	-	3	3	-	-
IT Hardware Asset Management Audit	9/29/23	High Risk	Completed	1	-	-	1	4	2	1	1
Identity and Access Management Audit	5/4/23	High Risk	Completed	3	3	-	-	1	1	-	-
Cybersecurity – PCs, Email and Internet	06/24/19	High Risk	Completed	5	4	-	1	4	4	-	-
Total Significant & Moderate Findings:				**19**	**8**	**1**	**10**	**14**	**10**	**1**	**3**

Contract Group Audits Q2 / FY25

Contract Audits Completed	
Audit Ratings	**No. of Audits Issued**
Low Risk	22
Needs Attention	1
High Risk	0
Total Audits Issued	**23**
Contract Audits In Progress	
Audit Types	
Interim / Close Out	1
Rate Reviews	5
Forward Pricing	0
Buy America / Special Request	0
Cost / Price Analysis	1
Change Orders	2
Total Contract Audits in Progress	**9**

- ✓ Identified Unallowable Cost in Overhead Rate Reviews as per Federal Acquisition Regulation (FAR) $32,676
- ✓ Identified Unsupported Costs in Cost/Price and Change Order Reviews $415,360.39

Fraud, Waste & Abuse Summary

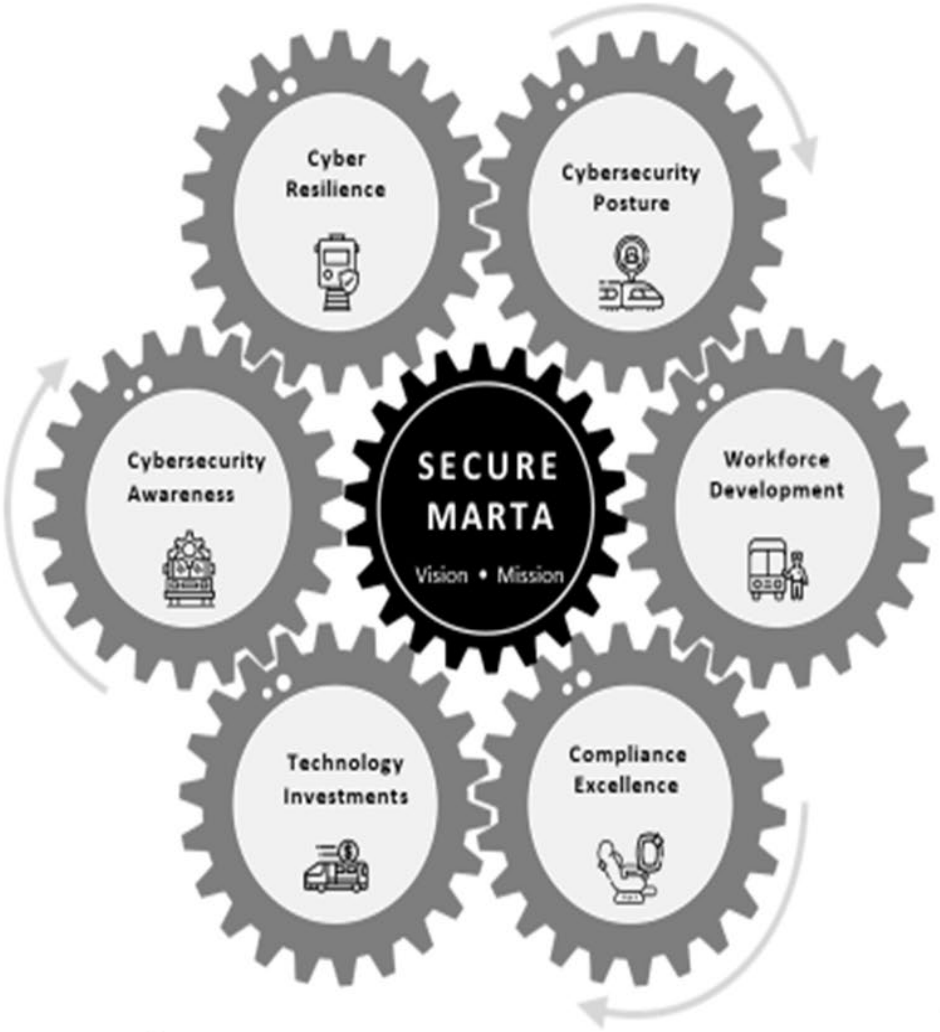
- Contract Compliance – not substantiated
- Timesheet reporting of excessive hours - substantiated
- Allegation of fraudulent documents and receipts on a p-card report - not substantiated
- D & I referral – Rail station supervisor time & attendance – in process
- Allegation of bid influence to favor a specific bidder – in process


marta
Bus
Stop
For Information: (404) 848-5000

Information Security Update
March 2025

marta

Strategic Priorities



Key Cybersecurity Threats Facing MARTA

1. **Phishing Attacks:** Attempts to compromise employee credentials.

2. **Ransomware:** Financial and operational risks from data encryption and extortion.

3. **Insider Threats:** Risks from both malicious and accidental employee actions.

4. **ICS/SCADA Vulnerabilities:** Risks to operational technology controlling trains and facilities.

5. **Third-Party Risks:** Weaknesses introduced by vendors and contractors.

Emerging Threats:

- AI-powered cyberattacks targeting transit systems.

- Increasing interest from sophisticated actors in Georgia's critical infrastructure

Key Focus Areas

1. **ICS/SCADA Security:**
• Integrating operational technology (OT) monitoring into cyber capability
• Focus on protecting critical infrastructure and addressing legacy system vulnerabilities.

2. **Cloud Migration and Management:**
• Transitioning enterprise applications and data storage to the cloud.
• Prioritizing data protection through secure access, encryption, and compliance.

3. **Vulnerability Management:**
• Implementing proactive vulnerability scanning and patching programs.
• Conducting penetration tests and vendor risk assessments to identify potential weaknesses.

Regulatory Compliance & Liability

1. Adherence to Federal Transit and Cybersecurity Regulations:

Compliance with FTA, TSA, and CISA cybersecurity directives is not optional; it is a prerequisite for maintaining operational funding and avoiding regulatory penalties. The Federal Transit Administration (FTA) mandates cybersecurity risk management as part of transit asset management, while the Transportation Security Administration (TSA) requires specific security measures for critical infrastructure.

2. CISA Cybersecurity Performance Goals:

Compliance with NIST 800-53 and NIST 800-82 in order to provide a structured approach to cybersecurity risk management. CISA's Cybersecurity Performance Goals (CPGs) establish baseline security expectations to build cybersecurity capability for critical infrastructure. Aligning with these standards strengthens our security posture and also demonstrates due diligence in the event of a breach, reducing liability exposure.

3. Third Party Risk Management &Contractual Security Obligations:

Many security breaches stem from third-party vendors and contractors with inadequate cybersecurity controls. Ensuring compliance with contractual security obligations, such as SOC 2 Type II, ISO 27001, and vendor cybersecurity assessments, is critical. Failure to enforce third-party security measures can lead to regulatory violations, data breaches, and potential liability claims under supply chain security regulations.

Artificial Intelligence and Machine Learning in Cybersecurity:

1. Faster Threat Detection & Response

AI helps us spot cyber threats in real time by analyzing patterns in our network. Instead of waiting for a hacker to cause damage, AI alerts us immediately, reducing downtime and keeping our transit operations running smoothly.

2. Preventing System Failures Before They Happen

Just like predictive maintenance helps us fix trains before they break down, AI can predict cybersecurity risks before they turn into major problems. This keeps our fare systems, train signals, and customer data safe from attacks.

3. Blocking Phishing & Scams That Target Employees

Cybercriminals often trick employees into clicking harmful links or giving away sensitive information. AI helps detect these scams faster, reducing the chance of a costly security breach caused by human error.

4. Stronger Security for Employee & Vendor Access

AI helps ensure that only the right people have access to critical transit systems. If an employee's account is acting strangely—like logging in from another country—AI can block access until we verify it's legitimate, protecting us from insider threats and hackers.

THANK YOU

Moving Cybersecurity Throughout the Authority