Integrated Mobility Division
N.C. DEPARTMENT OF TRANSPORTATION

BUILDING A CULTURE OF SECURITY:

CYBERSECURITY BASICS FOR TRANSIT IN NC

A plain-language primer on Operational Technology (OT) cybersecurity for agencies of every size

NCDOT IMD | SEPTEMBER 2026

Welcome & Today’s Agenda

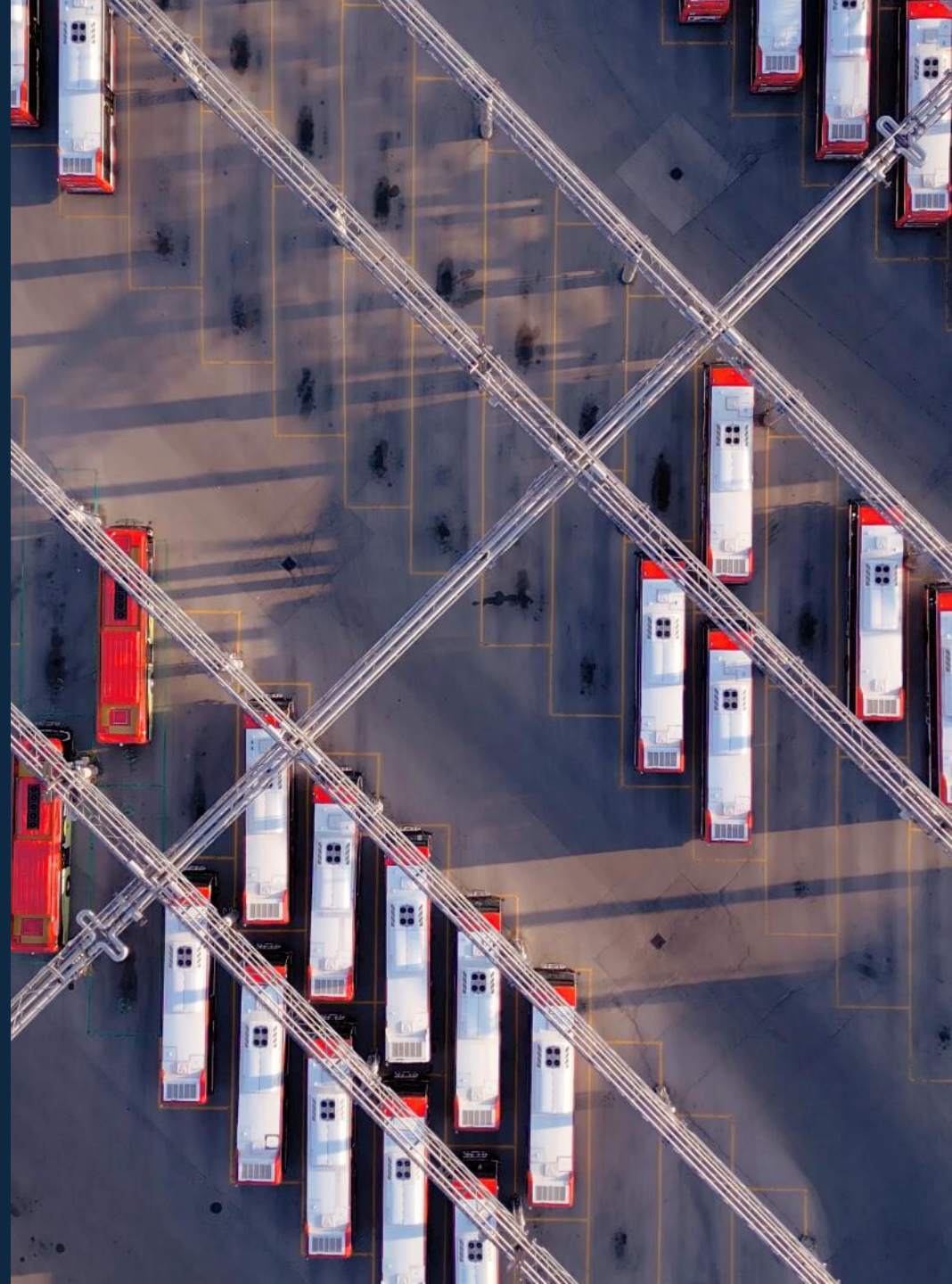
Why we’re here

Most transit training covers finance and safety. Today we add cybersecurity to the leadership toolkit.

What we’ll cover (45 minutes)

- What OT cybersecurity is — in plain language
- Why it now matters for FTA-funded transit
- Real incidents here in North Carolina
- What FTA expects — and how it differs by agency
- Practical first steps for any size agency

How to engage: live Q&A and a parking lot at the end.



The Context

SB 26-02
JULY 2026

Transit Cybersecurity Events

Purpose

The Federal Transit Administration (FTA) is issuing this Safety Bulletin to raise awareness of a cybersecurity advisory from the Cybersecurity and Infrastructure Security Agency (CISA). FTA *encies to review the information, assess whether it applies to their systems,* *eps to mitigate potential vulnerabilities. CISA's Cybersecurity Advisory* */www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.*

ilant against cybersecurity threats. Both state actors and non-state risk to U.S. critical infrastructure, including public transit systems. ks on transit agencies highlight the need for transit agencies to bilities and update response and recovery plans to address evolving

of Investigation (FBI), and several other co-authoring federal agencies y Advisory: *Iranian-Affiliated Cyber Actors Exploit Programmable Across U.S. Critical Infrastructure.*

nsit agencies to review the full advisory that details how advanced targeting internet-facing operational technology devices. For more ersecurity readiness, please visit FTA's Cybersecurity Resources for

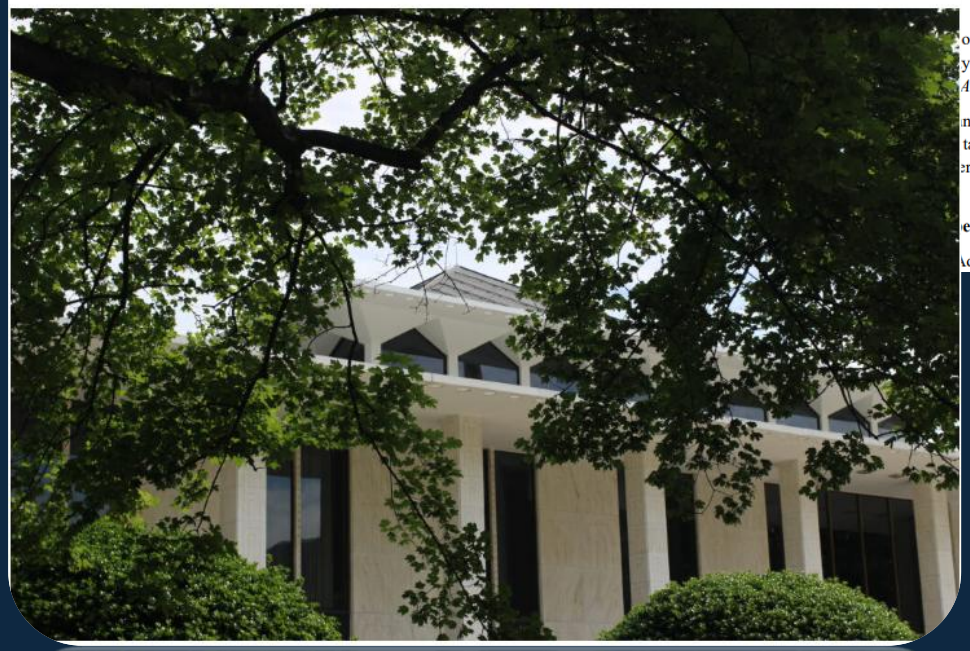
ersecurity Advisory

dvisory identifies affected products, including Rockwell

After North Carolina cyberattacks, IT officials warn General Assembly of poor preparedness

The state's systems face more than 10 billion attack attempts each month, a top cybersecurity official told lawmakers.

BY **BRANDON KINGDOLLAR** - FEBRUARY 5, 2026 5:53 PM



JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA26-097A

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

Publication: April 7, 2026

Federal Bureau of Investigation
Cybersecurity and Infrastructure Security Agency
National Security Agency
Environmental Protection Agency
Department of Energy
United States Cyber Command – Cyber National Mission Force

Integrated Mobility Division
N.C. DEPARTMENT OF TRANSPORTATION

What Is OT Cybersecurity?

OT = Operational Technology

In transit, OT includes:

- CAD / AVL (dispatch & vehicle location)
- Scheduling & trip-booking / demand-response software
- Fareboxes & mobile ticketing
- Two-way radio & communications
- Cameras & facility access
- Fuel management & vehicle telematics

✅ If these fail → service is impacted

What OT Looks Like at Your Agency

Rural

- Trip-booking / scheduling software
- Dispatch phones & two-way radio
- Fareboxes or fare app
- A few cameras; office network
- Fuel card / small fuel system

Small Urban

- CAD/AVL & real-time bus tracking
- Garage HVAC, fueling, bay doors - Supervisory Control and Data Acquisition (SCADA)
- Camera & access-control systems
- Mobile ticketing / fare network
- Vehicle telematics fleet-wide

Urbanized + light rail

- Signaling & train control
- Full SCADA / traction power
- Operations Control Center (OCC)
- Enterprise fare & comms networks

Why This Matters Now

Cyber threats are increasing across transit systems

Regulators (TSA, FTA) are tightening expectations

Cyber is now an operational resilience issue — not just IT

Integrated Mobility Division
N.C. DEPARTMENT OF TRANSPORTATION

Who This Applies To

Same FTA expectation — two different paths to it. Know which one is yours.

Directly Reviewed by FTA

Triennial Review

- 23 urbanized Section 5307 recipients (e.g., CATS)
- Reviewed by FTA every three years
- **Cybersecurity is now its own scored review area**
- Must show a real cyber risk-management process

Covered Through NCDOT

Triennial & State Management Reviews

- Rural/small Section 5311 & 5310 subrecipients
- Counties, non-profits, turnkey operators
- **No individual FTA review of your agency**
- NCDOT is reviewed on subrecipient oversight — expectations reach you via NCDOT policy

Two doors to the same room — both need a real, usable cyber program.

Takeaway #1

Cyber Risk = Service Risk

- **Key idea:** OT cybersecurity is about operations, not just data

- IT cyber = data → OT cyber = dispatch, buses, fares, comms
- A cyber event can cause:
  - Service disruption
  - Safety constraints
  - Reputational damage

- Leadership question:

  👉 *“What systems, if disrupted, stop service?”*

It Already Happened Here

Real Incidents

Cyberattacks are surging across North Carolina

- Record 2,349 data breaches reported in NC in 2025; hacking drove ~77%
- **Thomasville, NC (2025):** ransomware shut down city systems for weeks
- **Durham City/County (2020):** attack hit shared systems, including 911 dispatch
- **Charlotte (CATS):** under active federal safety oversight — how fast an agency lands under FTA scrutiny
- County-level attacks (e.g., near Anson County) hit small agencies least ready to respond

Resilience angle: when Hurricane Helene took down mountain-county communications, comms down is comms down — weather or attacker.

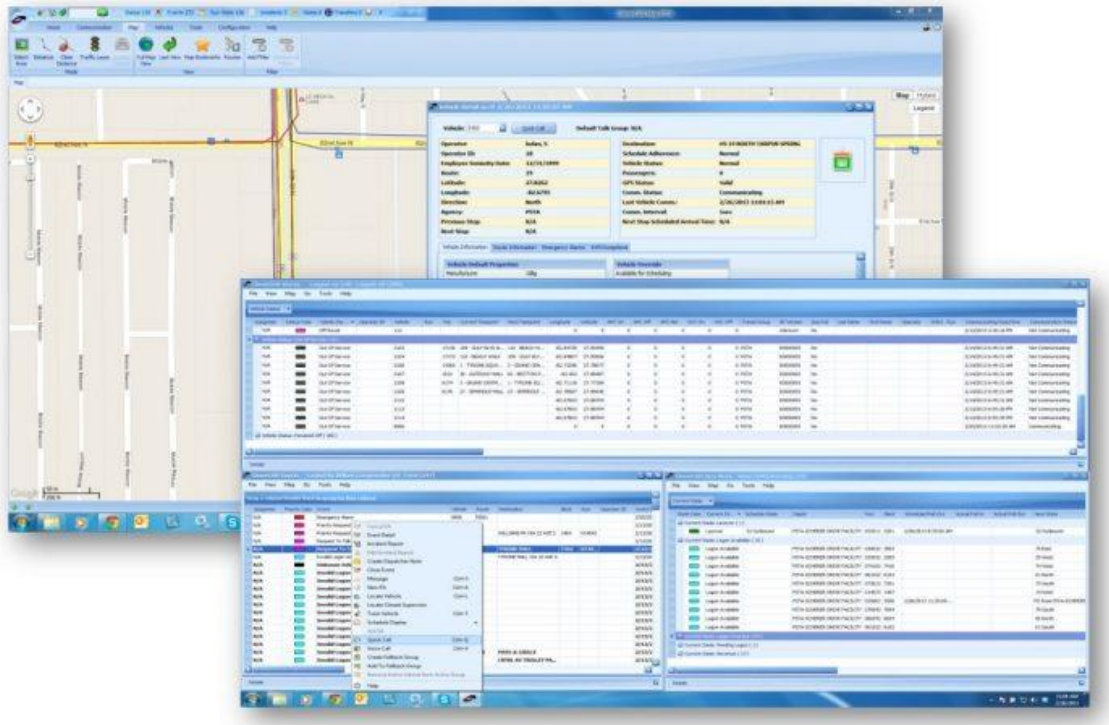
If it can hit a city hall or a county, it can hit a transit operation.

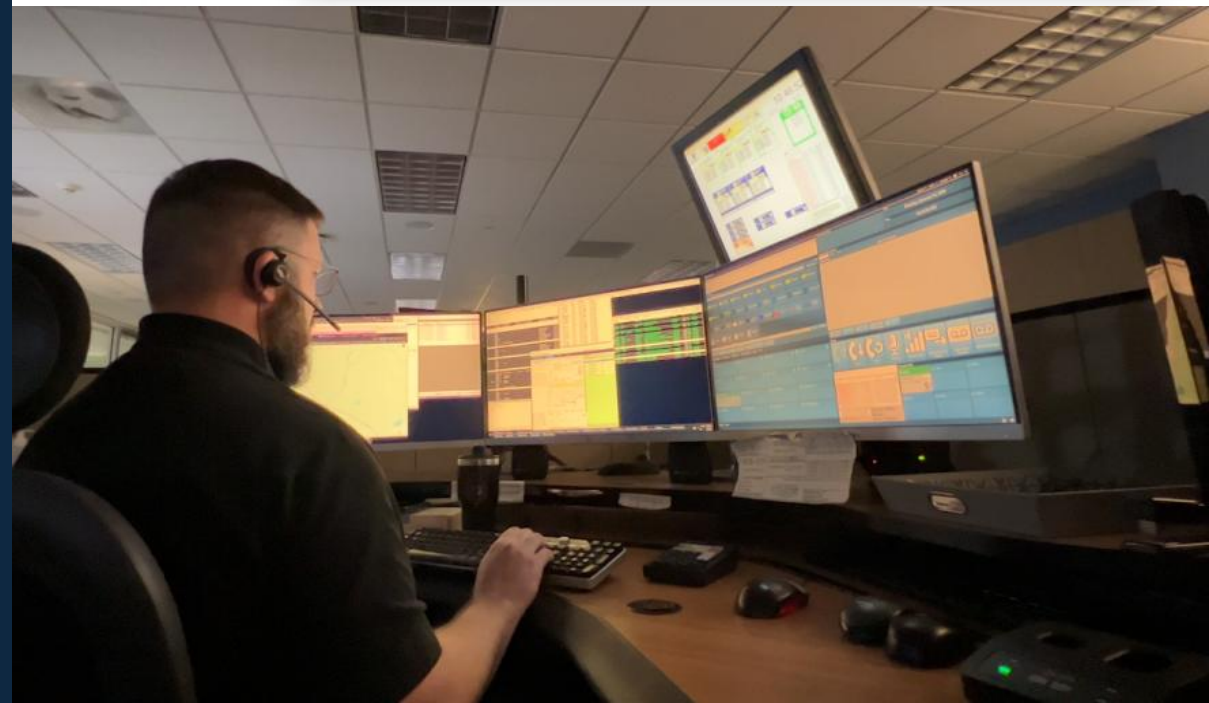
Takeaway #2

Protect What Matters Most

Key idea: Focus on the “crown jewels”

- Start with **asset visibility**
- Prioritize critical systems (not everything equally)
- Apply fundamentals:
  - Network segmentation (IT vs OT)
  - Controlled remote access
  - Monitoring & detection
  - Backups & recovery





Leadership Translation

What leaders should ask:

- Do we know our critical OT assets?
- Can IT issues spread into operations?
- Who has remote access to our systems?
- Can we detect issues quickly?

👉 **You don’t need tools first — you need clarity and control**

Integrated Mobility Division
N.C. DEPARTMENT OF TRANSPORTATION

Takeaway #3

Resilience is Practiced – Not Written

Plans don't matter if they aren't exercised

Cyber incidents = **operational incidents**

Response involves:

- Operations
- IT / Cyber
- Safety
- Communications
- Executives

Include vendors and maintainers

What to Practice

Run realistic scenarios:

- Ransomware affecting operations
- Loss of control center visibility
- Vendor account compromise
- Communications outage

Measure success:

- Detect → Isolate → Communicate → Recover

A “Cultural” Shift - Cybersecurity is not a bolt-on

It is becoming a **core engineering + leadership discipline**

Converging with:

- Safety
- Operations
- Capital programs

👉 **From compliance → to operational resilience**

Leadership Takeaway

"OT cybersecurity is not a firewall project. It is a leadership responsibility."

Govern the risk

Protect critical systems

Practice the response

👉 *Keep the system running. Keep the public moving. Keep trust intact*

Q&A, Parking Lot & Resources

Keep the Conversation Going

- Ask now: poll questions and live Q&A — no question is too basic
- Parking lot: we'll capture what we can't finish today and follow up
- Ongoing Q&A: a standing channel for FTA review questions and regulations
- Stay connected: regional check-ins with your NCDOT grant representatives

You don't have to figure this out alone.