CDTA COMMITTEE AGENDA

Strategic and Operational Planning Committee

Thursday, June 18, 2026 | 11:00 AM

Microsoft Teams & 110 Watervliet Ave

Committee Item	Responsibility
Call to Order	Michael Criscione
Approve Minutes of Thursday, May 21, 2026	Michael Criscione
Administrative Discussion Items	
• Security Overview	Rich Fantozzi

Next Meeting: Thursday, July 23, 2026, at 11:00am via Microsoft Teams and 110 Watervliet Ave.

Adjourn	Michael Criscione

Capital District Transportation Authority
Strategic and Operational Planning Committee
Meeting Minutes – May 21, 2026, at 10:55am; via Microsoft Teams and 110 Watervliet Ave.

In Attendance: Jayme Lahut, Jackie McDonough, Patrick Lance; Frank Annicaro, Amanda Avery, Chris Desany, Jaime Kazlo, Gary Guy, Jon Scherzer, Patricia Cooper, Stacy Sansky, Mike Williams, Thomas Guggisberg, Dave Williams, Sarah Matrose, Jack Grogan, Lance Zarcone, Rich Cordero, Emily DeVito, Kelli Schreivogl, Steve Wacksman

Meeting Purpose
Regular monthly meeting of the Strategic and Operational Planning Committee. Board Member Jackie McDonough noted that a quorum was present. Minutes from April 23, 2026, meeting were reviewed and approved.

Administrative Discussion Item
- CDTA's on-time performance (OTP) has improved significantly over the past decade, following a strategic shift in 2014 toward more data-driven scheduling and a goal of reaching 85% OTP. Performance climbed into the high 70% range by 2021, but beginning in FY22 the system experienced a sustained decline. This downturn was driven largely by post-pandemic workforce challenges and rapid service expansion, including new BRT lines and service in Montgomery and Warren Counties.

- In response, we partnered with Courval Scheduling (CSched) in 2023 to evaluate and strengthen scheduling practices. This effort focused on leveraging AVL data for more precise run times, improving data quality, and applying disciplined scheduling fundamentals such as realistic layovers and more efficient route pairing. Staff were trained on these methods, and a phased rollout began in 2025, starting with Albany service and later expanding to Troy.

- These changes have begun to yield results. We have seen our first sustained improvements in OTP since 2021, with systemwide performance increasing approximately 4–5%. Gains have been strongest in areas where the new scheduling approach has been fully implemented.

- Some challenges remain, particularly in Albany, where changes in traffic conditions—such as reduced speed limits and increased enforcement—have eroded some of the early gains and require continued recalibration.

- Looking ahead, we are expanding optimized scheduling practices to additional service areas, including Schenectady, Saratoga, and Glens Falls, with work now largely led by internal staff and supported by CSched. Continued refinement of run times and alignment of service levels will be essential to sustaining and building on recent improvements.

Next Meeting
Thursday, June 18, 2026 at 11:00am via Microsoft Teams and at 110 Watervliet Ave.

Current State of CDTA IT Security

Strategic & Operational Planning Committee 6.18.2024

CDTA

CDTA.ORG

Operational Risk

Why Cybersecurity Matters to CDTA

Transit operations depend on technology

Scheduling, dispatch, CAD/AVL, radio, fare systems, customer communications, facilities, cameras, and business systems all rely on secure and available IT services.

Cyber incidents create business impact

A cyber event can affect service reliability, customer trust, employee productivity, emergency response, insurance availability, regulatory compliance, and public reputation.

Security is enterprise resilience

The program's objective is not just to block attacks. It is to keep the authority operating, recover quickly, and preserve trust during disruption.

Security is now part of Operational Continuity, not just Defend and Protect.

Overview

Current Environment

Environment	Total
Users	175
Servers	114
Wireless Access Points	115
End User Computers	309
Mobile Devices	240
Fixed Cameras	397
Network Smart Devices (IoT)	800+
Bus Routers	396
Mobile Cameras	1297
Bus Devices (Farebox, Signs, DVR)	1980

Take Aways

- The CDTA technology environment keeps growing and changing as the authority grows.
- IoT devices are becoming a large target for hackers and security needs to be reviewed with each system.
- Buses are becoming more integrated with our network and security posture.

Overview

Current Environment

Environment	Total
Users (all environments)	272
Email (90 days)	1.8 Million
Teams Messages and Calls	205,800
One Drive	1.5 Million
Share Point	1.3 Million
Data Storage (On Site)	100 TB
Data Storage (Cloud)	45 TB

Take Aways

- Access includes not employees but all 3rd parties who have access to any environment that we manage.
-
- Employees carry access with them at their homes and on their mobile devices.
- Communications is still the main entry point for attackers.

Risk Context

Current Threats

- Credential theft, phishing, ransomware, cloud account compromise, and vendor compromise remain common attack paths.
- Public-sector and transportation organizations remain attractive because they operate essential services and interconnected systems.
- Cloud identity, remote access, third-party integrations, and unsupported systems are high-value targets.
- Cyber insurance, audit expectations, and executive accountability continue to rise.

Take Aways

- Attackers are faster, more automated, and increasingly focused on identity and trusted access.
- We are evaluating risks against what attackers are doing now, not what traditional perimeter security was built to stop.

AI Threats

Artificial Intelligence: Risk Accelerator

- AI makes phishing and impersonation more realistic, targeted, and scalable.
- Synthetic text, voice, and images can increase fraud and social-engineering risk.
- AI can help attackers automate reconnaissance and summarize public information about targets.
- AI can reduce the skill barrier for understanding vulnerabilities, scripting attacks, and refining intrusion paths.
- Unsanctioned AI use can create data leakage risk if sensitive information is pasted into public tools.

Take Aways

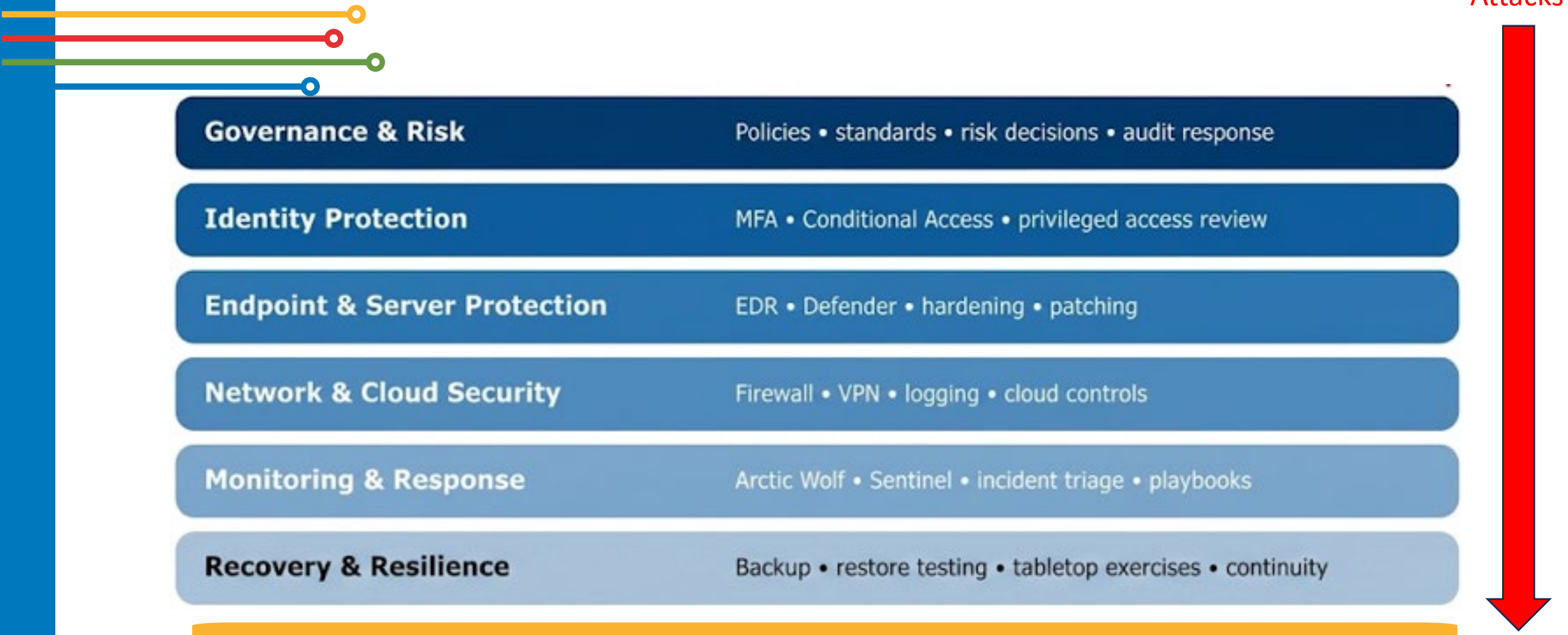
- AI makes existing cyber risks faster, cheaper, and more convincing rather than creating new ones.
- We are treating AI as part of the security risk management program, not just a technology innovation.

Security Program at a Glance

Identity	Microsoft Entra ID, MFA, Conditional Access, account monitoring
Endpoint	SentinelOne, Microsoft Defender
Network	Palo Alto firewalls, VPN controls, network monitoring
Vulnerability	Tenable scanning, SLA review, remediation tracking
Monitoring	Arctic Wolf SOC, Microsoft Sentinel, endpoint and cloud telemetry
Awareness	KnowBe4 simulations, Phish Alert reporting, user training
Recovery	Veeam, Pure Storage, DR and backup capabilities
Governance	Policies, SOPs, tabletop planning, vendor access controls

CDTA's security program is layered, monitored, and increasingly risk-based.

Layered Defense Model



Detection, response, and recovery, not just prevention, determine operational impact.

Major Control Areas

Identity and Access Protection

- Securing employee logins is now our first line of defense for cloud, remote access, email, and many business applications.
- CDTA uses extra sign-in verification and rules that automatically block risky logins (MFA and Conditional Access) to reduce the chance of accounts being taken over.
- Privileged accounts, executive accounts, vendor access, and temporary exceptions require higher scrutiny.
- Future work focuses on reducing repeated failed-login attempts and keeping logins secure even after sign-in, especially when something looks unusual.

Take Aways

- The likeliest attack path is a stolen employee login, not a breached firewall.
- Privileged access review, vendor access registration and review, application consent and strong lifecycle controls are all in place.

Major Control Areas

Security Monitoring and Incident Response

Monitoring Coverage

Arctic Wolf, our outside security partner, watches for threats around the clock.
Activity from our laptops, servers, email, cloud sign-ins, and firewalls all feeds into this monitoring (SentinelOne, Microsoft Sentinel, Microsoft 365, Entra, and Palo Alto).

Critical Alerts: 1.28 Minutes

Non-Critical Alerts: 13.43 Minutes

Response maturity

How we sort alerts, investigate, follow up on weaknesses, handle incidents, and escalate them is becoming more structured and measurable.

90 Days: 821 Alerts

Next steps

Tabletop exercises, executive communications, business continuity alignment, and a coordinated enterprise incident response model.

Fast detection and coordinated response reduce the operational impact of incidents.

Risk Reduction

Employee Awareness and Phishing Readiness

- Phishing simulations and awareness training continue to improve employee readiness.
- AI-based simulations increased difficulty, better reflecting the current threat environment.
- Employee reporting is an important detection source, not just a compliance metric.
- The program should continue emphasizing reporting behavior, not just failure avoidance.

Take Aways

- With training and easy reporting, employees become an early-warning system.
- 20% increase in messages reported over last year. Total of 6,409 reported since April of 2023.
- 77,778 phishing emails sent since 2020. Only .7% clicked a simulated phishing test (Phish Prone Percentage).

CDTA.ORG

Risk Reduction

Vulnerability and Patch Management

- Regular automated scans (Tenable) identify security weaknesses across our systems and support ongoing review.
- The most serious findings are reviewed based on how severe they are, how easily they could be exploited, how critical the affected system is, and how feasible a fix is.
- Patch management requires coordination with operational systems, vendor-managed platforms, and approved maintenance windows.
- The program is moving toward stronger documentation, tracking against our fix-by deadlines, monthly reporting, and consistent enforcement of written procedures.

Take Aways

- We are remediating issues faster than ever, Critical and High within 10 days, and tracking updates for auditability.
- When immediate fixes would disrupt operations, the program prioritizes, applies protective workarounds, and documents the plan.
- Track recurring issues and finding ways to fix them long term.

2026 Vulnerabilities	6,109	
Patched within 10 Days	4,607	75%
Critical within 10 Days	908	88%
High within 10 Days	3,421	76%

External Validation

OSC Audit and Continuous Improvement

Audit outcome

The OSC security audit identified one finding related to delays in applying High-severity patches beyond the defined SLA.

Remediation

The delayed High findings had already been remediated.

Process improvement

We strengthened and enforced patch-management SOP expectations to reduce recurrence and improve accountability.

An external audit raised one patch-management finding, now remediated and built into stronger procedures.

Risk Overview

Data Protection and Compliance

- Sensitive information protection requires policy, employee behavior, monitoring, and access governance.
- Microsoft Purview/DLP capabilities help identify potential exposure of protected information, but tuning and workflow maturity are important.
- Email security, encryption practices, legal/eDiscovery roles, and mailbox delegation controls require ongoing review.
- AI adoption increases the importance of clear rules for what data may be used in AI tools and agents.

Take Aways

- Data protection takes governance, training, and access control, not a single technology.
- Using technology today to find and categorize protected information.
- Email encryption for protected information will be the next major data protection milestone.

Risk Overview

Operational Systems and Legacy Risk

- Transit operations rely on interconnected systems such as dispatch and vehicle-tracking (CAD/AVL), radio, cameras, fare collection, scheduling, websites, and customer-facing applications.
- Some critical platforms may include older operating systems, vendor-managed servers, specialized equipment, or upgrade constraints.
- Security work must be balanced with operational availability and coordinated maintenance windows.
- Legacy risk should be tracked through criticality, vendor ownership, patch status, compensating controls, and modernization plans.

Take Aways

- Operational technology risk is enterprise risk because it can disrupt service delivery.
- Project Plans are place for all systems including INIT, Spear and Genfare.

Risk Overview

Vendor and Third-Party Access

Why it matters

CDTA depends on vendors for core transit platforms, hosted systems, maintenance, remote access, integrations, and specialized support.

Risks

Vendor access can become an attack path if accounts, VPN profiles, exceptions, consents, or remote-support workflows are not tightly governed.

.

Next Steps

Maintain a vendor access registry, temporary-access tracker, MFA validation, access review cadence, and owner-based exception disposition.

Vendor and trusted access must be granted and reviewed like privileged access.

Risk Overview

AI Governance

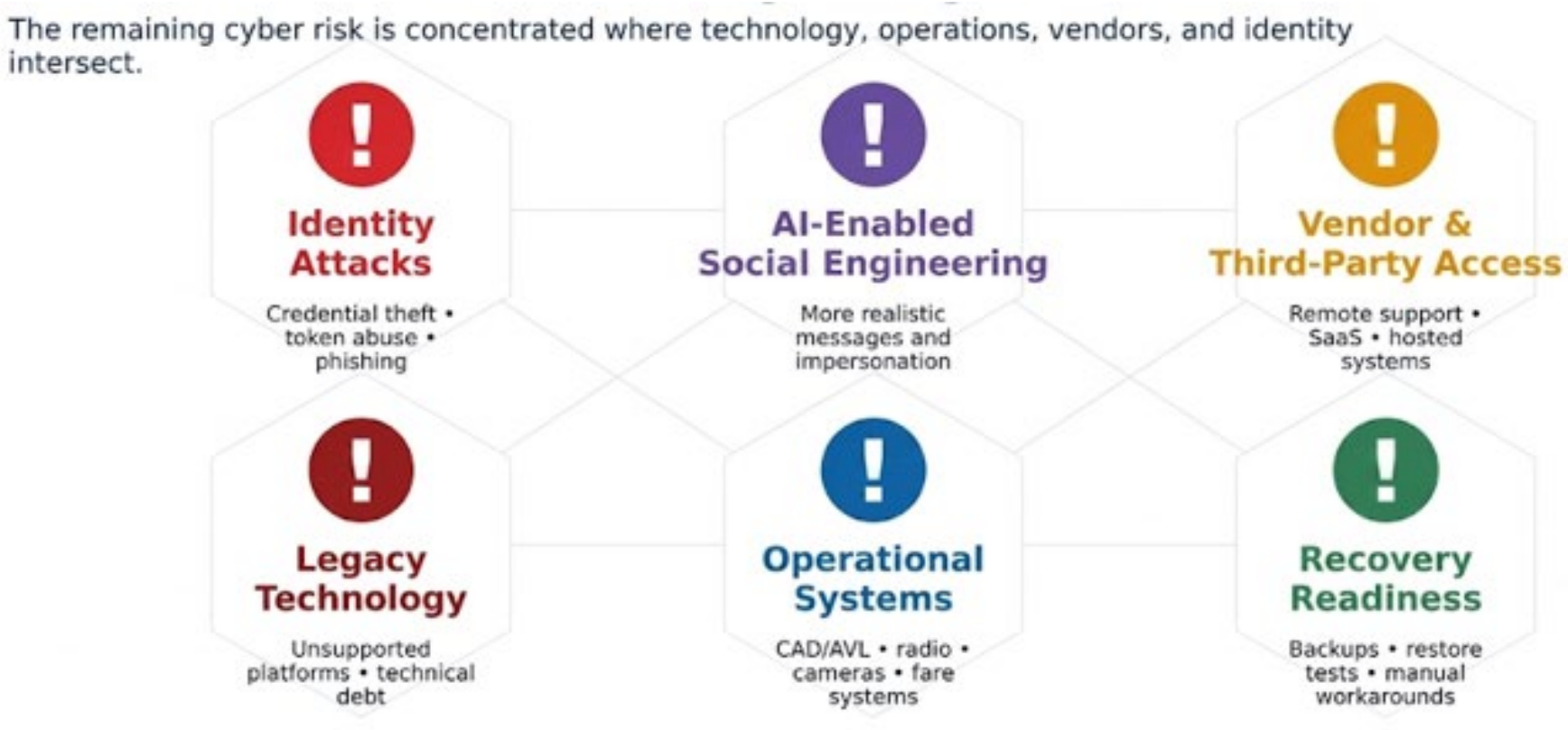
Human review	AI supports review; staff make final decisions.
No changes without sign-off	AI never patches, disables, or changes live systems on its own; staff approve every action.
Evidence-based outputs	Findings reference reports, logs, or source data.
Logging and traceability	Agent actions and outputs remain auditable.
Limited access	Agents access only approved repositories and data.
Data boundaries	Sensitive information stays within approved platforms and workflows.

AI adoption stays controlled through approved use cases, clear data boundaries, human oversight, and measurable controls.

Risk Summary

Current Risk Areas

CDTA's biggest risks now cluster where identity, vendors, and operational technology intersect, not at the network edge.



CDTA.ORG

Future

Security Roadmap

Near-term

Continue vulnerability remediation and reporting; tighten Conditional Access; improve DMARC/SPF enforcement; formalize vendor access review; complete tabletop planning.

Mid-term

Conduct tabletop exercises; improve asset criticality; formalize temporary exceptions; mature incident playbooks; improve security dashboards and monthly metrics.

Strategic

Align to NIST CSF 2.0; govern AI adoption; reduce legacy exposure; improve resilience for critical transit systems; sustain investment in monitoring, identity, backup, and staff capability.

The next phase focuses on governance maturity, resilience, response readiness, and continued risk reduction.

Takeaways

- CDTA's security posture has materially improved through layered controls and stronger monitoring.
- Cybersecurity is an operational resilience issue, not only an IT issue.
- AI is both a risk accelerator and a defensive opportunity; controlled adoption is the right posture.
- The OSC audit result shows a maturing program that remediates findings and strengthens procedures.
- Continued governance, investment, and cross-department support are needed to manage cyber risk as enterprise risk.

THANK YOU!

Questions? | Comments? | Next Steps.

CDTA

CDTA.ORG