

STRATEGIC AI POLICIES

Managing Risk While Driving Government Efficiency and Innovation

Tas Jalali, CISO, AC Transit

Chair, AI Subcommittee, APTA



“

In a sprawled environment, attackers do not need to subvert defenses – they exploit the absence of governance.

Applied AI Governance — Tas Jalali

TODAY'S AGENDA

01



Where transit agencies are most vulnerable

02



Technology tools that create boundaries

03



Helping leaders use AI responsibly

04



Managing pushback

05



Managing up, down, and sideways

THE THREE AI ATTACK SURFACES



The AI You Know

ChatGPT, Claude, Gemini — standalone tools at employee desktops. Addressed with acceptable use policies. Necessary but insufficient.



The AI You Can't See

AI embedded inside existing SaaS platforms — enabled by default, invisible to inventories. Sprawl by contract.



The AI That Acts

Agentic AI that chains actions across systems at machine speed — modifying records, sending emails, executing workflows.

Most agencies are only watching for the first one.

THE VISIBILITY GAP

21%

of organizations maintain
a current AI agent inventory

Akto 2025

40%

of enterprise apps will include
AI agents by end of 2026

Gartner 2025

119%

growth in agents deployed

Salesforce 2025



“Shadow IT was a cost and compliance nuisance. Agent Sprawl is an operational existential threat.”

— *Applied AI Governance*

TRANSIT-SPECIFIC VULNERABILITIES



OT Convergence

AI tools interact with dispatch, vehicle tracking, fare collection, and maintenance systems. A scheduling agent that modifies routes affects real-world operations and rider safety.



Unclassified Data

PII, ADA accommodation data, financial records, security feeds — no classification layer means AI cannot distinguish a fare summary from individual rider disability information.



Vendor-Managed AI

Scheduling platforms, customer service systems, predictive maintenance tools — deployed and managed by vendors outside agency governance and visibility.



Accountability Gaps

When an AI agent causes harm, no single individual specified the sequence of actions. Regulators do not accept diffused accountability.

THE EXECUTION BOUNDARY

Where reasoning becomes action



This is where governance must be enforced — before an action produces irreversible consequences.

“*The most persistent misconception in enterprise autonomy is the belief that governance can remain centralized purely in IAM. In reality, governance must live at the execution boundary, because that is where intent becomes effect.*”

— *Applied AI Governance*

FIVE CONTROLS THAT CREATE BOUNDARIES

1

Discovery & Inventory

Network-level AI API traffic detection, NHI credential inventory, SaaS platform audits

2

Enforcement Gateway

Governed boundary where identity is verified, policy evaluated, and permit/deny/escalate rendered

3

Policy-as-Code

Governance rules as executable logic — versioned, tested, enforced at runtime, not PDF documents

4

Kill Switch & Containment

Egress filtering, rate limiting, progressive containment — halt agents through technical controls

5

Evidence Infrastructure

Structured audit records produced as a byproduct of enforcement, not manual reporting

THREE QUESTIONS EVERY AGENCY MUST ANSWER

INVENTORY

Do we know what AI agents are operating in our environment?

JUSTIFY

Can we explain and justify the actions those agents take?

CONTROL

Can we stop them if we need to?



“IAM owns identity, applications own action, security owns risk — and no team owns governance at runtime.”

— Applied AI Governance

MAKING IT REAL: TRANSIT SCENARIOS

ADA Compliance Failure

A paratransit scheduling agent optimizes routes but does not account for ADA accommodation data stored in a separate system. The schedule is operationally efficient but non-compliant.

Privacy Violation

A customer service AI responds to a rider complaint by pulling incident records and including the names of employees involved. The response is helpful, detailed, and a privacy violation.

Procurement Bypass

A maintenance prediction tool flags a component and automatically generates a purchase order above the procurement threshold — bypassing approval because the vendor's AI operates outside the governance layer.

“*Threat modeling for agentic AI must assume that material harm can occur without a classic breach.*”

— *Applied AI Governance*

MANAGING PUSHBACK

“You’re slowing us down.”

Governance must match the speed of technology. Low-risk use cases complete in days, not months. Proportional governance — not every case needs the same scrutiny.

“Other agencies are already doing this.”

Ask them: Do they have an inventory? Can they produce an audit trail? Can they halt an agent in under an hour? If no — they have unmanaged risk, not innovation.

“The vendor said it was secure.”

Vendor attestation is not agency governance. We ask: what data is processed, where is it stored, can we revoke access, can we audit actions?

“It’s just for internal use.”

You can shut down a rogue Shadow IT server with minimal business impact. You cannot easily shut down a rogue agent that has negotiated 1,000 refunds, fired 3 employees, or reconfigured a firewall.

MANAGING UP, DOWN, AND SIDeways



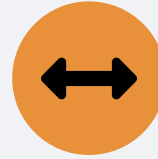
BOARD & EXECUTIVES

Lead with liability, not technology. “If one of our AI systems causes harm, can we demonstrate controls were operating?” 75%+ of CISOs report personal concern about AI liability.



STAFF & TECHNICAL

Cultural debt accumulates when speed is praised but restraint is invisible, and when exceptions are celebrated as “getting it done.” Embed controls in the pipeline — enforced automatically, not added as paperwork.



PEERS & DEPT HEADS

Reframe from permission to accountability. Every AI agent gets a named human sponsor. “I’m not here to slow you down. I’m here to make sure you have the evidence when this goes to the board.”



Autonomy is not inherently unsafe.

Ungoverned autonomy is.

Applied AI Governance — Tas Jalali



Available on Amazon

QUESTIONS & DISCUSSION

Tas Jalali

CISO, AC Transit | Chair, AI Subcommittee, APTA

[linkedin.com/in/tasawarjalali](https://www.linkedin.com/in/tasawarjalali)