Darwin

EXECUTIVE BRIEFING · 2026

A CISO'S PLAYBOOK

A CISO's approach to solving *AI governance*.

A practical brief on bringing AI use into view and under control inside government, written for security leaders working under real-world constraints.

In partnership with Nancy Rainosek

Former State Chief Information Security Officer · State of Texas

CONTENTS

What's *inside*.

SECTION 01 — CONTEXT

AI adoption is already happening inside government—approved or not.

Employees are using AI tools to move faster, solve problems, and reduce manual work, often outside official systems, policies, or visibility.

A difficult position for CISOs.

For security leaders, this creates a hard balancing act. **The risks are real, but so is the pressure to enable progress.** Blocking AI outright is rarely an option; ignoring it is worse.

The conversation has moved past whether agencies should allow AI. What matters now is whether they can **see, guide, and manage it** as adoption accelerates.

The question has changed.

The challenge is no longer deciding whether to allow AI.

It is figuring out how to manage it while it is already in motion—across employees, teams, and workflows that the security organization has not been part of approving.

> *"By the time governance is on the agenda, adoption is already on the desktop."*
>
> NANCY RAINOSEK · FORMER STATE CISO, TEXAS

SECTION 02 — THE PROBLEM

The biggest risk is not the technology —it's not seeing how it's used.

Employees may upload sensitive data into public tools without understanding the implications. Teams adopt solutions without procurement or security review. Over time, entire workflows emerge that remain invisible to IT and security.

A hidden compliance surface.

The visible layer of AI inside an agency; sanctioned pilots, enterprise licenses, formally procured tools, is rarely where the meaningful exposure sits. The exposure is in the long tail of personal accounts, free-tier products, and embedded features quietly switched on inside existing software.

None of this shows up on a security dashboard. None of it appears in a procurement record. And yet every interaction may produce a record the agency is obligated to retain, review, or produce on request.

> *"You cannot govern what you cannot see."*
>
> NANCY RAINOSEK · FORMER STATE CISO, TEXAS

Visibility is the prerequisite, not the goal. Without it, every other control — policy, training, retention, review — operates on incomplete information. **Establishing what AI is already in use, and where, is the first move worth making.**

SECTION 03 — IN PRACTICE

Governance is an *operational discipline*, not a policy exercise.

A written policy is necessary but insufficient. Governance only works when it lives in how teams actually operate—day to day, tool to tool, decision to decision.

- Coordinated ownership. Security, IT, legal, and business teams share accountability, not a single gatekeeper. Effective programs distribute decisions to the people closest to the work, with security as a partner rather than a chokepoint.
- **Continuous, not one-time.** Monitoring replaces a single approval gate; posture changes as usage does. A tool's risk profile on day one is not its risk profile six months in.
- Enabling, not blocking. The goal is safe, accountable adoption aligned with agency priorities, providing approved alternatives, not just denying access to everything employees want to try.

> *"Security should not be the roadblock. It should be a partner in responsible AI adoption."*
>
> NANCY RAINOSEK · FORMER STATE CISO, TEXAS

SECTION 04 — FRAMEWORK

Four moves that *build on each other*.

A practical sequence for moving from no visibility to durable governance. Each step depends on the one before it, the order matters as much as the work.

1 FOUNDATION

A living inventory of AI systems.

Catalog every tool, approved or not. The inventory is the foundation for visibility, control, and everything that follows and it has to update itself as adoption shifts.

2 ACCOUNTABILITY

Clear ownership for every system.

Business units own how tools are used. Security owns how risk is managed. No system without a name attached and no decision deferred because no one is sure who decides.

3 PROPORTIONALITY

A risk-based lens that scales.

Not every use case carries the same sensitivity. Tier controls to impact so governance scales with adoption instead of collapsing under the weight of treating every tool the same.

4 ENFORCEMENT

Controls backed by real mechanisms.

Restrict unsafe tools, enable approved alternatives, and require human oversight where the stakes demand it. Policy without enforcement teaches employees that the policy is optional.

SECTION 05 — THE SHIFT

AI governance is not a *future-state* problem.

The window to approach AI governance proactively is open now. Agencies that wait for adoption to settle will find themselves managing risks they never had the opportunity to shape.

Adoption is bottom-up.

It is no longer driven solely by formal programs or top-down initiatives. It moves through individuals, teams, and external pressures — faster than traditional oversight can keep up with.

Visibility, ownership, and operational governance matter now — not as a complete solution, but as a starting point for bringing AI use into view and under control.

The agencies that move first.

The agencies that recognize this early will be better positioned to adapt as AI capabilities evolve — not because they predicted what was coming, but because they built the muscles to respond.

Those that wait may find themselves responding to risks they never had the opportunity to manage, in conditions chosen by vendors, employees, and circumstance.

> The opportunity is not to "solve" AI governance — it's to make sure governance moves at the same pace as adoption, instead of trailing it by months or years.

THE BOTTOM LINE

AI is not waiting for *governance* to catch up.

The question for leaders is not whether their organization will adopt it—but whether they will be able to see it, guide it, and manage it as it becomes part of everyday operations.

If your team is working through how to approach AI governance in practice, Darwin can help you think through the next steps ; from inventory and ownership through proportional controls and enforcement.

Talk with our team →

Watch the full webinar

Nancy Rainosek Former State Chief Information Security Officer, State of Texas, in partnership with Darwin.

Darwin