# The Federal Government in the Age of AI

## *Innovation, Security, & Oversight*

### A Strategic Overview of 2025

Regulatory Changes | Technical Solutions | Policy Debates

Synthesis of 2025 Congressional Hearings, FedRAMP Rev 5 Updates, and Industry Analysis.

# Executive Summary: The State of Federal AI in 2025

## The Regulatory Baseline

Transition to FedRAMP Revision 5 is the new standard. Shift from static checklists to a Threat-Based Methodology aligned with the MITRE ATT&CK framework.

## The Technical Solution

Agencies are moving toward Retrieval-Augmented Generation (RAG) and “AI Factories” to ground AI in agency data without exposing sensitive intel to public models.

## Adoption Velocity

Major shifts in 2025: DoD’s “GenAI.mil” deploying to 3 million personnel; FDA adopting agentic AI for review workflows.

## The Critical Tension

A collision between the “DOGE” initiative’s push for radical deregulation and grave concerns from cybersecurity experts regarding data centralization.

# The Strategic Context: A Race for Adoption

The U.S. advantage in innovation is being eroded by bureaucratic inertia.

## The Challenge

- China's Semiconductor Fund: $47.5 Billion
- R&D Investment (2024): $500 Billion
- Infrastructure: Controls >60% of global 5G base stations

## The U.S. Context

**Strategic Weakness:** Slow bureaucratic adoption vs. integrated state strategy.

**Testimony**: Yll Bajraktari (SCSP) calls for a "Technology Competitiveness Council" modeled on the Space Race.

**Critical Insight:**

This is not just a competition of invention, but of adoption.

# The New Framework: FedRAMP Revision 5

Modernizing the baseline to match the threat landscape.

---

## Supply Chain (SR Family)

New control family addressing third-party risks and provenance.

## Privacy Focus

Mandatory privacy impact analysis (CM-3) and training (AT-3).

**Threat-Based Methodology**

## Red Teaming

Mandatory for Moderate & High baselines. Simulates advanced real-world attacks.

## Encryption

FIPS 140-validated encryption required for ALL data-at-rest and data-in-transit.

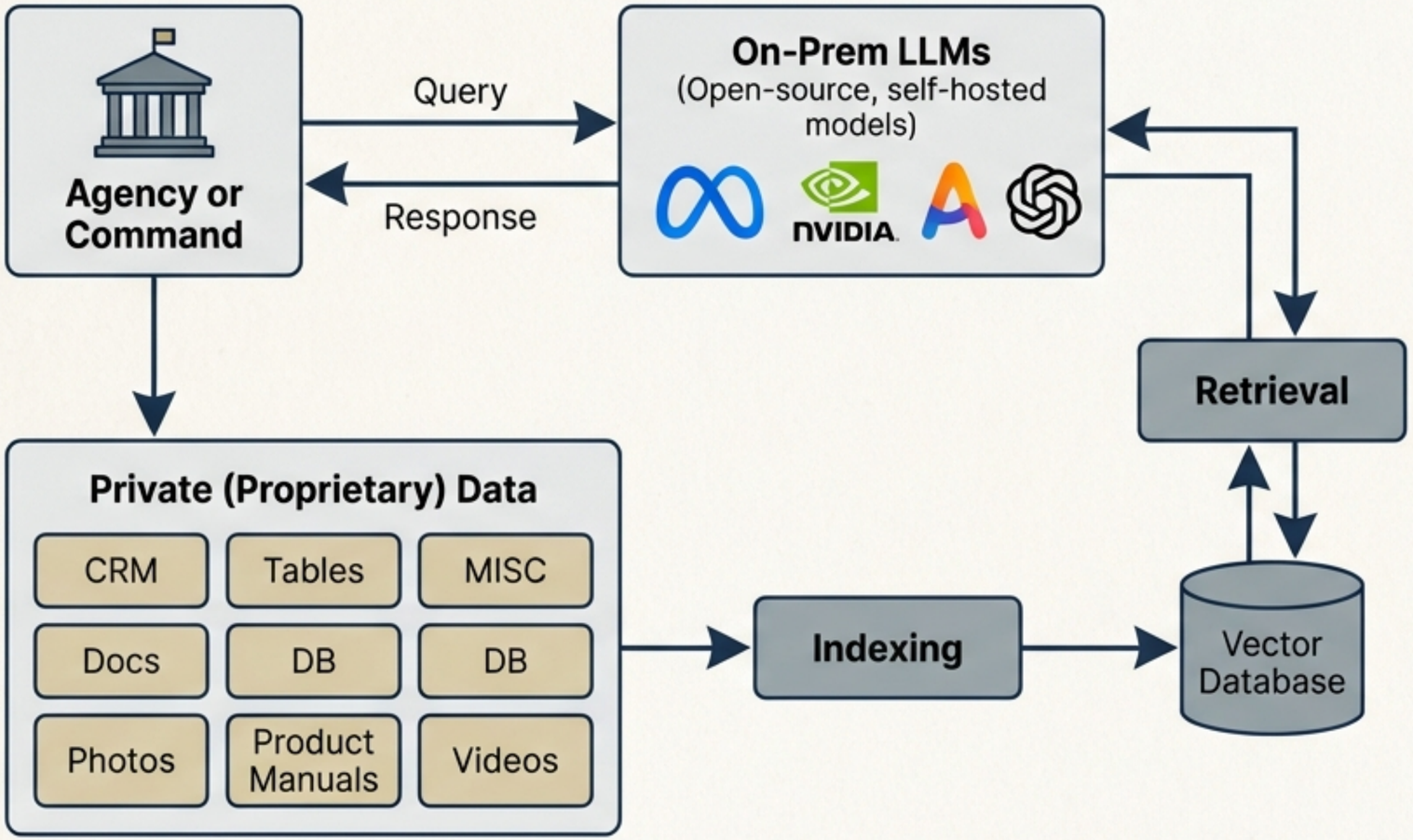
# Transitioning to Rev 5: The Compliance Timeline


**Strategic Shift:** Emphasis on customization and tailoring controls to specific risks rather than “one size fits all’.

Source: Schellm

# Operationalizing AI: The ‘RAG’ Advantage

Grounding answers in agency data without retraining models.




## The Value Proposition

**Data Sovereignty:** Data stays in secure enclaves; model does not learn or leak.

**Accuracy:** Answers grounded in documents with citations.

**Speed:** Policy updates reflected instantly without retraining.

# Trusted Infrastructure: The Government ‘AI Factory’

- **The AI Factory Pipeline**
  - Ingest –> Index –> Retrieve –> Generate
- **Hardware Requirements**
  - **Manufacturing:** US-Designed / US-Made (Supply chain transparency).
  - **Compute:** NVIDIA RTX PRO 6000 & HGX systems.
  - **Compliance:** IPv6 ready, CMMC 2.0, FIPS 140-3 cryptography.

# Deployment at Scale: 2025 Milestones

Google Public Sector achievements in Defense and Health.

## Defense (DoD)

- **Deployment:** ‘GenAI.mil’ serving 3 million personnel.
- **Capability:** IL6 authorization for Secret classified data and air-gapped appliances.

## Health (FDA)

- **Deployment:** Agentic AI workflows assisting reviewers.
- **Milestone:** First GenAI assistants (Gemini) to achieve FedRAMP High.

**Theme:** Moving beyond ‘GovCloud’ constraints to accredited commercial cloud.

# The Human Element: Augmentation & Efficiency

*"The question is not whether the Federal Government should adopt AI. It is whether we will lead or follow."* — Bhavin Shah, Moveworks


**ROI (City of Glendale)**

Saved 3,500 employee hours.


**Reduction in Help Desk Requests**

Honeywell Case Study.


**Employee Scale Support**

Broadcom scaled 10k to 50k without adding support staff.

# The Oversight Debate: Innovation vs. Bureaucracy

## The Problem

**Legacy Spend:** $100 Billion+ annually, with 80% going to legacy systems.

## The FedRAMP Tax


## The Proposals

- **Regulatory Sandboxes:** Allow controlled testing.
- **FIT Procurement Act:** Raise acquisition thresholds to $500k for faster pilots.
- **DOGE Perspective:** A necessary shock to dismantle “sludge” regulation.

# The Oversight Debate: Privacy & Security Risks

The danger of ‘Sloppy’ Innovation and Data Centralization.

**Data Exfiltration**
(“Preparing the battlefield”)


**Coercion**
(Leverage against officials)

**Poisoning**
(Bad data input)

## Testimony: Bruce Schneier

**Warning:** Centralizing data creates a single target for adversaries. Privacy Act of 1974 is outdated for the AI age.

**Controversy:** Allegations of stripping security controls and handing master databases to private firms (Palantir).

# Voices from the Floor

Key Testimony Highlights from the Hearing

## On Efficiency

"The question is not **whether the Federal Government** should adopt AI. It is **whether we will lead or follow**."

**— Bhavin Shah**
(Moveworks)

## On Risk

"Sacrificing cybersecurity in an effort to create an AI future not only risks the country... it risks all of us."

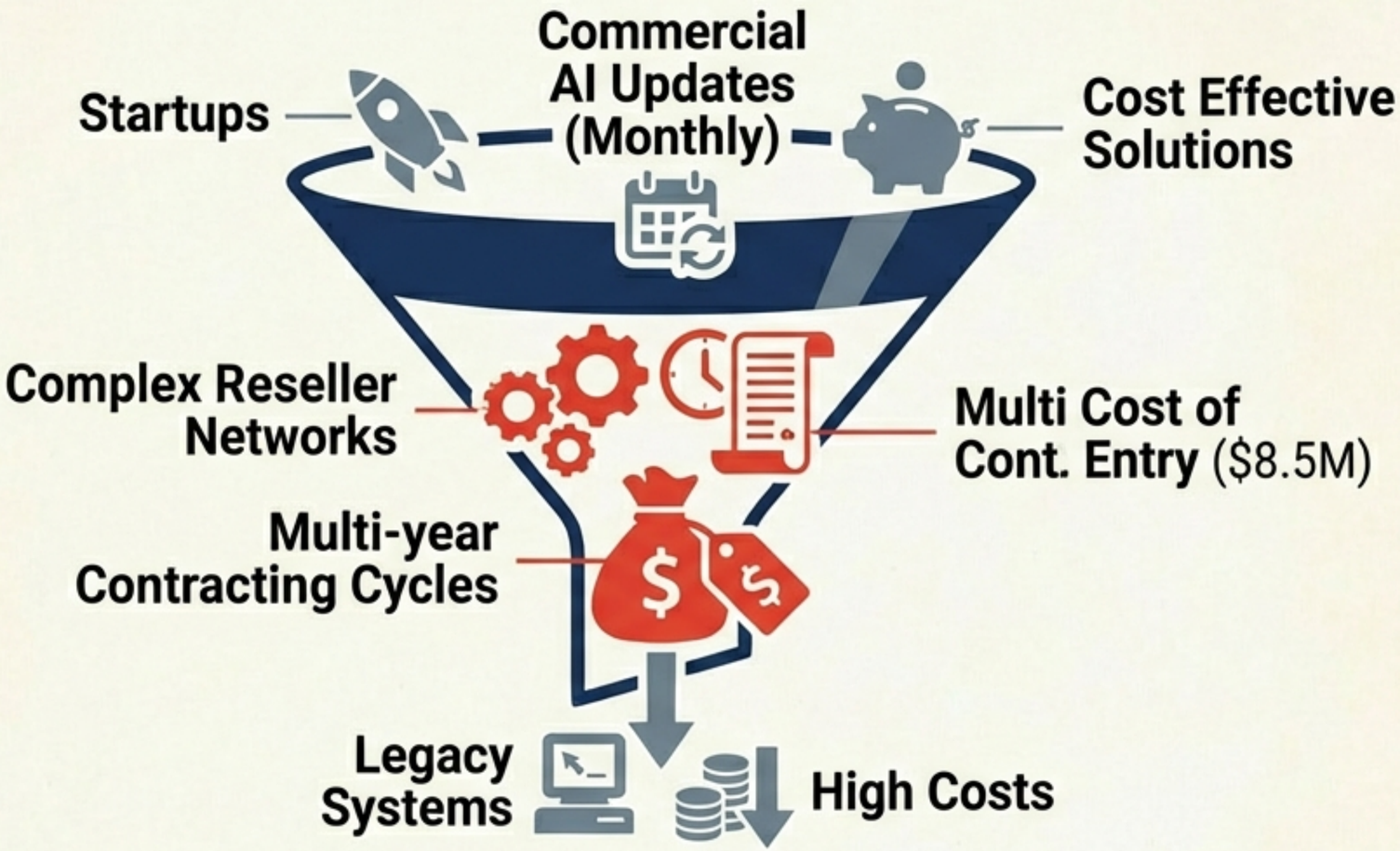
**— Bruce Schneier**
(Harvard Kennedy School)

## On Fraud

"The bad guys have all our data... proactive investment is needed."

**— Linda Miller**
(TrackLight)

# Procurement: The Bottleneck to Innovation




## Proposed Fix

**Innovator Programs:** Allow startups to bypass reseller webs for pilot deployments.

# Strategic Recommendations for Agency Leaders

## 01 Modernize Baselines

**Modernize Baselines.** Transition to FedRAMP Rev 5 immediately to align with the threat landscape.

## 02 Adopt RAG Architectures

**Adopt RAG Architectures.** Utilize retrieval-based systems to secure data enclaves while leveraging commercial LLMs.

## 03 Overhaul Procurement

**Overhaul Procurement.** Establish regulatory sandboxes and raise acquisition thresholds to pilot innovation faster.

## 04 Defensive Posture

**Defensive Posture.** Assume adversaries have exfiltrated data. Prioritize data integrity and resilience.

# Conclusion: The Pivot Point

The technology is ready: Commercial Cloud, RAG, AI Factories.

The rules are defined: FedRAMP Revision 5.

The Challenge: Balancing the speed of disruption with ‘Zero Trust’ safeguards.

**The barrier is no longer technical. It is procedural.**