# Congressional Testimony

## Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity

Thursday, June 12, 2025, at 10:00 a.m. EDT in 310 Cannon House Office Building

**Chairman and distinguished members of the subcommittee,**

Thank you for the opportunity to testify. I am here representing Securin, a CISA JCDC member, and with deep roots in federally funded research organizations, collaboration with DARPA, the Department of Defense, Arizona State University, New Mexico Tech, and Mississippi State University. Securin is not just another cybersecurity startup; we have taken research from the lab to the marketplace, building patented technology that uses AI for early warning and predictive defense, empowering organizations to stay ahead of attackers. One of our notable projects is CACTUS - Computational Analysis of Cyber Terrorism Against the US.

I have had the privilege of serving in various governmental roles. My perspective today is shaped particularly by my seven-year tenure as the Chief Technology Officer for the State of Arizona. This experience has provided me with a profound understanding of the technological policy challenges faced at both the state and federal levels.

Let me start and end with one core message: **Securing AI models is not just about protecting algorithms—it is foundational to America's national and economic security, with national resilience against adversaries ranging from nation states to individual detractors.**

For example, recent APT campaigns, such as those attributed to Volt Typhoon, have exploited toxic combinations of vulnerabilities - 'toxic combos' - chaining together weaknesses in both legacy and AI-powered systems to achieve persistent, stealthy access.

Despite industry pledges, we continue to see critical weaknesses like CWE-20, improper input validation, in major AI and MCP server deployments. Multiple vendors have released products with these flaws, and our data shows these are among the most exploited weaknesses in the wild.

Uniquely, our research reveals that as AI models become more capable, their attack surface grows. Models with higher reasoning ability are paradoxically more exploitable, making robust model security and adversarial testing essential as we advance AI capabilities.

As AI becomes the backbone of our economy, healthcare, and critical infrastructure, its vulnerabilities become the vulnerabilities of our entire society.

## Why This Matters Now

- **Offensive AI:** Both attackers and defenders are leveraging AI to simulate sophisticated cyberattacks, from nation-state operations to ransomware schemes, exposing vulnerabilities in real-time. This offensive strategy is not just valuable - it's indispensable for organizations using AI in cybersecurity to outpace adversaries.

- **Weaponization at Speed:** Attackers are already using AI to automate phishing, generate deepfakes, discover vulnerabilities, and create polymorphic malware that evades traditional defenses.

- **Global Competition:** We observe a stark contrast between Chinese and Western AI models: Chinese models often outperform in raw speed and scale, but Western models tend to prioritize security and transparency. This performance-security tradeoff is a critical consideration for U.S. policy and competitiveness.

---

## Why Now: The Urgency of AI Guardrails

The threat landscape is evolving rapidly. Nation-state actors and ransomware groups are not waiting for legislation - they are exploiting every gap and inconsistency. AI-powered attacks are already undermining authentication, public trust, and critical infrastructure. The rapid proliferation of AI has magnified old vulnerabilities and introduced new ones, from supply chain risks to adversarial manipulation of models.

Secure by Design principles, initially established in 2005 by DHS's Software Assurance Forum and NIST, are still highly pertinent today, yet their consistent integration into AI is insufficient. Despite industry pledges, recurring critical vulnerabilities, such as CWE-20 (improper input validation), persist in significant AI and MCP server deployments. Several vendors have launched products with these deficiencies, which are currently being exploited.

---

## The Regulatory Landscape: Complexity and Opportunity

Securin's NAVIGATE framework allows us to assess the effectiveness of AI bills across the country in a way that is accessible to both policymakers and the public. We have reviewed hundreds of bills and found significant regional variation:

- **California's SB-1047** emphasizes robust governance and annual reviews, while states like New Mexico and Colorado offer more basic frameworks with limited guidance and lower scores for training and integration support.

- **Reporting timelines and sector-specific requirements** vary widely - some states require employee education, some don't; some have 72-hour reporting, others 90 days.

- **Health use** is the most legislated category (112 bills), followed by government and criminal use, highlighting the sectors most at risk.

This patchwork creates a maze for organizations operating across state lines, increasing compliance costs and leaving potential security gaps.

---

## The Path Forward: Federal Baseline with State Partnership

A one-size-fits-all federal law could overlook local needs, but leaving it to states alone risks fragmentation and weak spots. What's needed is a federal baseline, much like PCI or HIPAA - developed in partnership with states, setting minimum standards while allowing for regional adaptation. Our NAVIGATE assessment shows that no state excels in every area; combining best practices is essential.

---

## Let me close where I began:

Securing AI is not just about algorithms - it is about protecting America's future.

1. **Securing AI models is foundational to national cybersecurity.** Offensive security - anticipating how AI can be weaponized - must guide both technology and policy.

2. **Urgent, enforceable guardrails are needed now.** Attackers are moving faster than regulators, so we must act quickly and precisely.

3. **A coordinated federal-state approach, informed by real-world offensive security insights and clear frameworks like NAVIGATE, is the only way to ensure both innovation and protection.**

Thank you!
I look forward to your questions and to working together on this critical mission.