



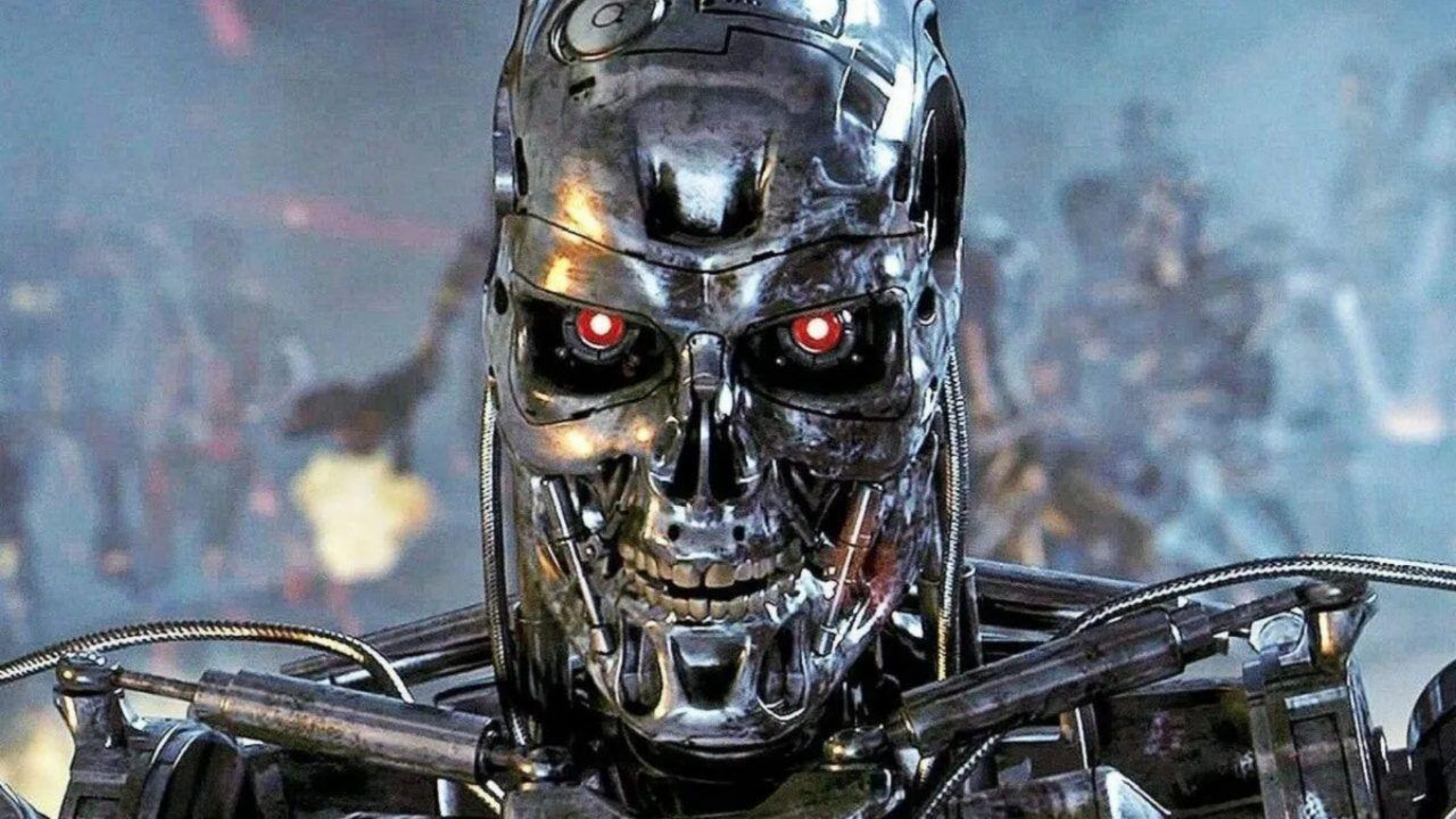
Artificial Intelligence: Is Your Bank Ready?

Anjelica Dortch

Vice President, Operational Risk &
Cybersecurity Policy

Modera, ND | September 2026





ANTHROPIC

- **Most Powerful Model:** Frontier model, not publicly available; gated behind Project Glasswing due to offensive risk
- **Zero-Day Discovery:** Autonomously found thousands of critical flaws across every major OS and browser; generates working exploits at 72% success rate, without human guidance
- **Scale of Impact:** Project Glasswing partners (200+ orgs, 15+ countries) identified 10,000+ high/critical severity vulnerabilities in critical infrastructure software
- **Anthropic's Warning:** Within 6–12 months, competitors will have Mythos-class models — potentially released without safeguards



OpenAI

- **Controlled Cyber Access:** GPT-5.5-Cyber released May 2026 under “Trusted Access for Cyber” program for vetted defenders only; requires phishing-resistant authentication
- **Attack Simulation Benchmark:** UK AISI found GPT-5.5 completed a 32-step simulated corporate cyberattack in 2 of 10 runs (Mythos: 3 of 10), confirming near-parity on offensive capability
- **Jailbreak Risk:** AISI red-teamers developed a universal jailbreak in 6 hours that bypassed GPT-5.5's safeguards across all malicious cyber queries in multi-turn agentic settings; AISI's 95-task offensive cyber benchmark fully saturated by frontier models as of Feb 2026



DeepMind

- **AI Threat Defense Platform:** Launched May 2026, uniting Gemini, Wiz, CodeMender, and Mandiant to autonomously discover, prioritize, and remediate vulnerabilities at machine speed
- **AI Agent Trap Research:** Identified 6 novel attack vectors targeting AI agents via malicious web content — invisible traps that hijack agentic AI without exploiting traditional software vulnerabilities
- **Real-World Threat Data:** Analyzed 12,000+ real-world AI-enabled attack attempts across 20 countries; maturing from experimental use to industrial-scale adversarial AI operations
- **CodeMender:** AI agent using Gemini to automatically find AND fix critical code vulnerabilities — the first full-cycle defense loop



THE THREAT TO COMMUNITY BANKS



- Adversaries with access to frontier-class models will soon have the capacity to probe core banking systems, online banking portals, and fintech APIs for vulnerabilities at scale, with limited human oversight.
- AI-generated phishing, synthetic identity fraud, and deepfake social engineering are no longer emerging threats and will continue to expand.
- Exploitation windows have collapsed from weeks to minutes. Third-party vendor risk is now AI-amplified.

AI Policy Landscape – Federal Level

Action Plan



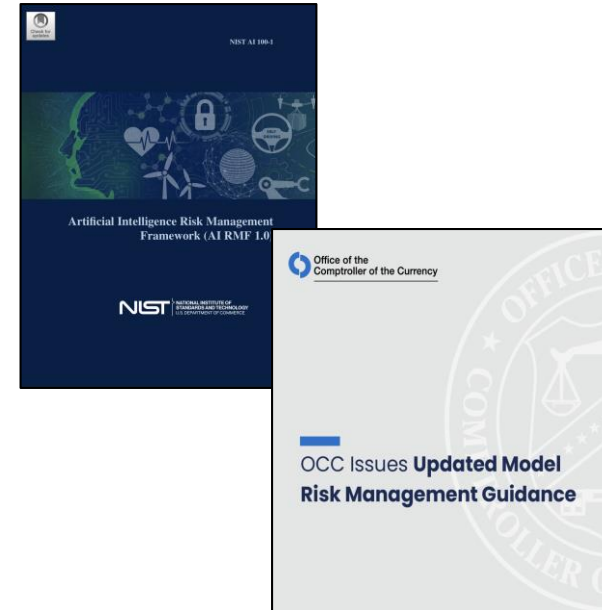
President Trump's AI Action outlines a framework to assert U.S. leadership in artificial intelligence, centered around three pillars: (1) Accelerate AI Innovation; (2) Build American AI Infrastructure; (3) Lead International AI Diplomacy & Security

Executive Order



President Trump signed the Executive Order on June 2, 2026, with an explicit callout of community banks as critical infrastructure operators. The order directs CISA within 30 days to facilitate access to cybersecurity tools and services for all community banks.

NIST & Treasury



The NIST AI RMF offers a voluntary framework for managing AI risks. Treasury's recent update to the Model Risk Management Guidance provides a considerations related to vendor and other third-party AI products for institutions over \$30 billion in assets.

Joint Trades Letter
Secure & AI-Ready
America Action
Plan

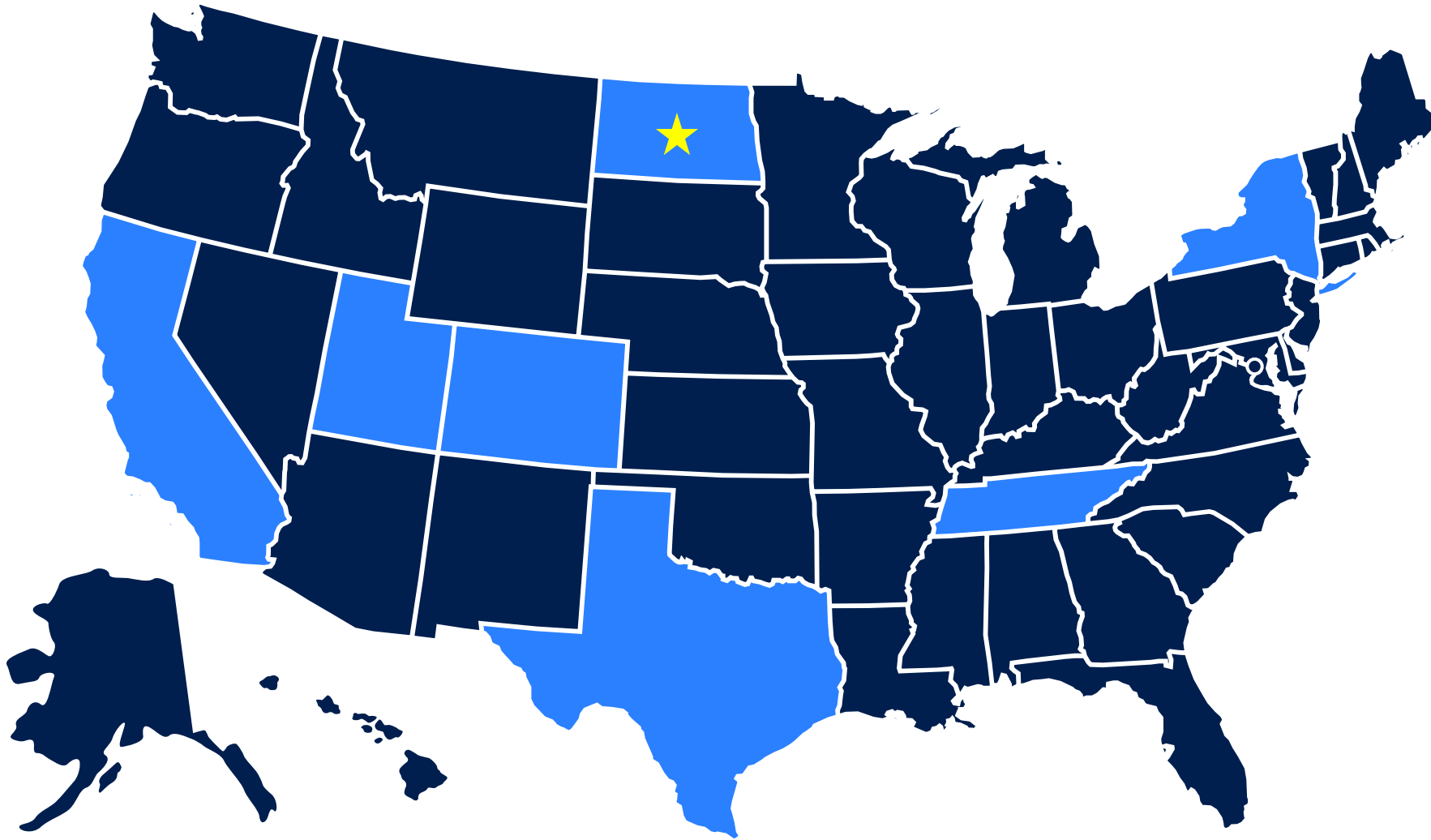
Letter on AI
Innovation in
Community
Banking



Completed Actions

AI Policy Landscape – State Level

As of the September 2026, over 2,000 AI-related bill have been introduced across 45 states



SB 24-205 – Colorado Artificial Intelligence Act



First comprehensive AI regulation in the U.S. that [mandates risk assessments](#) and documentation for developers & deployers of high-risk AI systems.

SB 53 – Transparency in Frontier AI Act



First-in-the-nation law that requires AI companies to reveal their [safety protocols](#).

New York AI Bills



These bills cover automated employment decisions, [consumer disclosures](#), AI transparency, and synthetic identify and deepfake concerns.

TX Reasonable AI Governance Act



Focuses on harmful or deceptive AI uses, deepfakes, and unlawful discrimination. Viewed as the [industry-friendly alternative](#) to CO & CA.

AI Policy Landscape - North Dakota Legislative Assembly

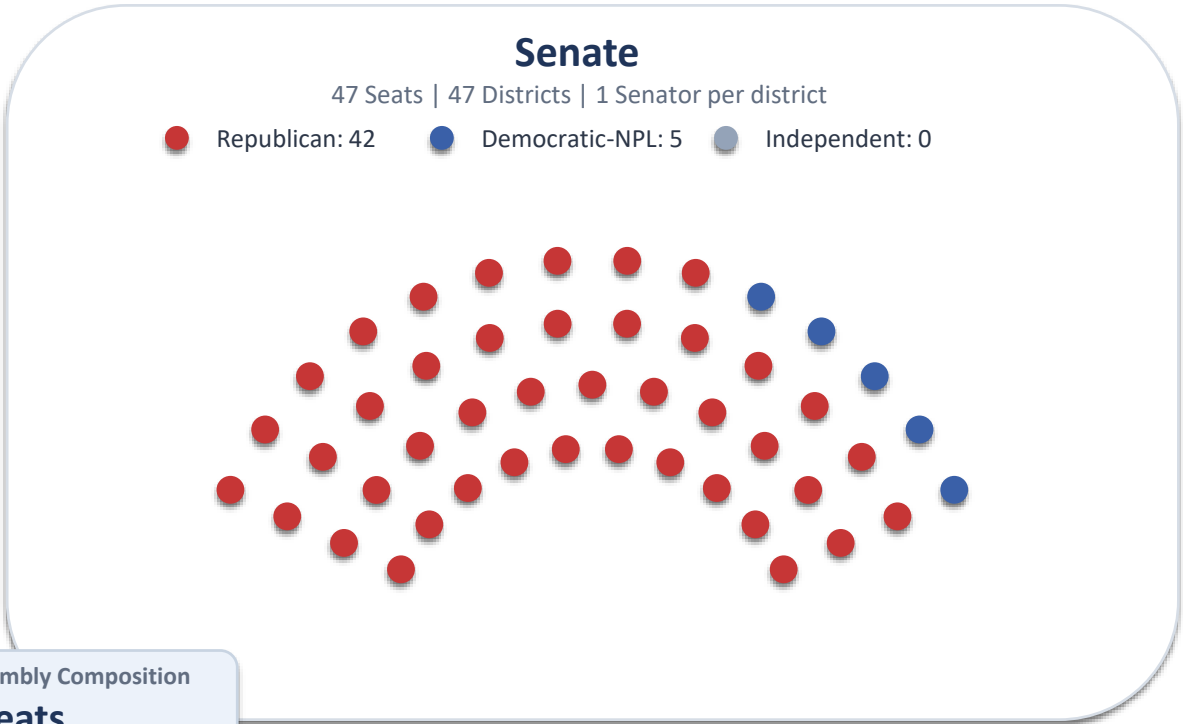
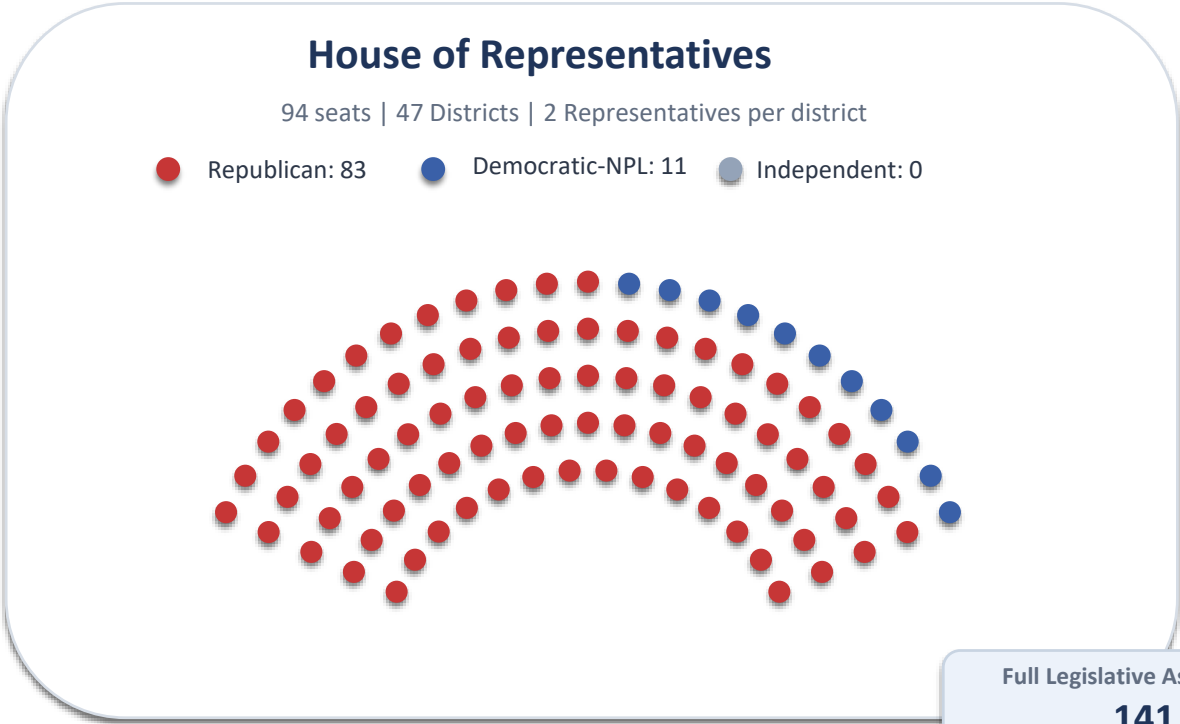
69th Legislative Assembly (2025–2026)

Governor

Kelly Armstrong

Lt. Governor

Michelle Strinden



Recent North Dakota AI Bills

Bill	Name	Status
HB 1167	Artificial intelligence disclosure statements in political communications	Passed
HB 1386	Certain computer-generated images involving minors (CSAM-related)	Passed
HB 1351	Sexually expressive images / deepfake-related protections	Passed
HB 1320	Prohibit deepfake videos and images	Failed

Source: North Dakota Legislative Branch - <https://ndlegis.gov/assembly/69-2025/regular>

CSBS AI Supervisory Framework

What the September 2026 announcement means for community banks

Bottom line

State examiners now have a practical framework to assess AI use, governance, and when existing supervisory tools should apply — without creating new legal obligations.

1. Expect AI questions in exams moving forward

Banks should be ready to explain whether AI is used in products, operations, compliance, fraud, customer service, internal support, or embedded vendor tools.

2. The AI Inventory becomes the starting point

The first exam conversation is likely to center on the bank's AI footprint: use case, owner, business purpose, data used, vendor involvement, and human review.

3. Risk-tiering will drive the depth of the review

Higher-risk uses — consumer outcomes, sensitive data, limited human oversight, significant reliance — call for stronger governance, testing, monitoring, and oversight.

Community Bank Action:

Start with a current AI inventory and risk-tiering worksheet; use proportional controls tied to the bank's size, complexity, risk profile, and actual AI use. Leverage ICBA resources to further educate staff on AI and data governance.

Conference of State Bank Supervisors



Artificial Intelligence Supervisory Framework

Core Examiner Guide

Conference of State Bank Supervisors

Version 1.0

Approval Date: August 13, 2026

Guide Contents

Considerations and Background	2
Overview	2
Initial Scoping	3
Document Request List	4
Governance and Oversight	5
AI Inventory and Use Cases	6
Generative AI and Emerging Use	7
Use of Existing Supervisory Resources	8
Third-Party and Vendor Review	8
Model Risk Review	8
Consumer Protection Review	8
Operational Risk Review	8

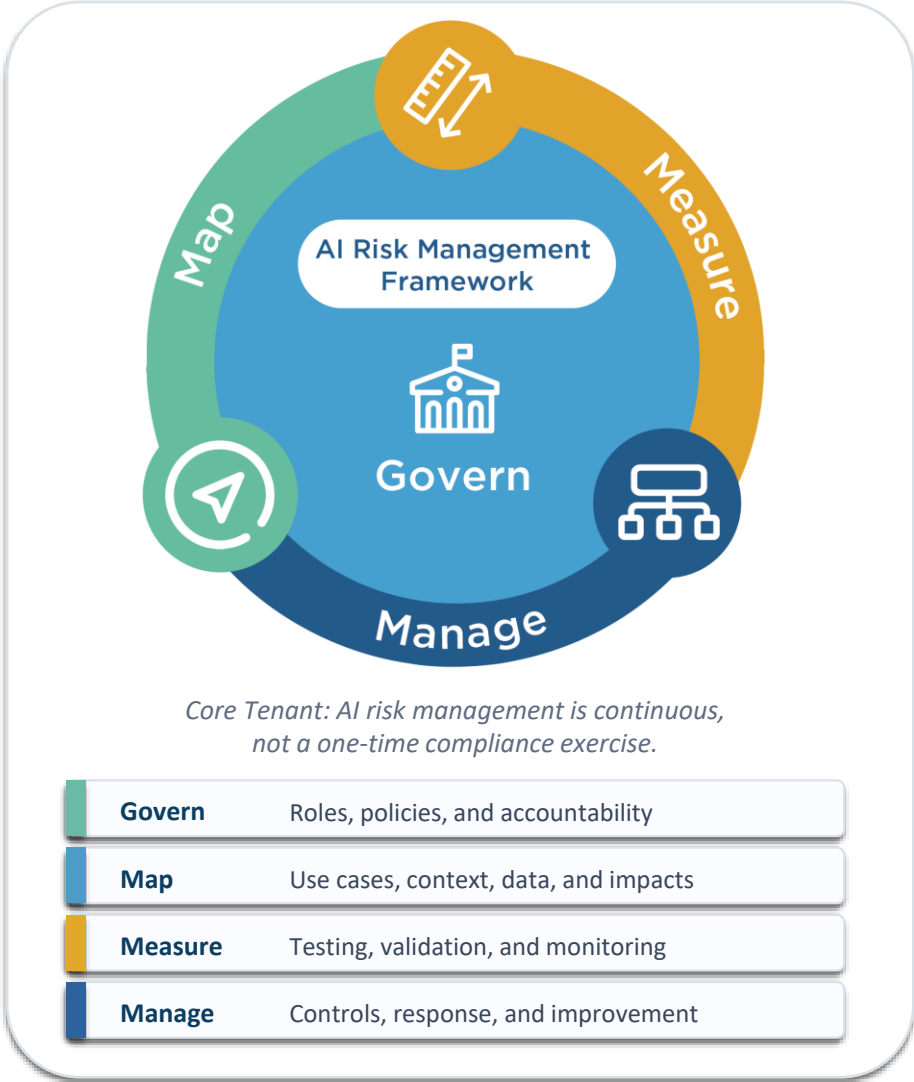
Version 1.0

Approval Date: 08/13/2026

Page 1 of 8

NIST AI Risk Management Framework (AI RMF)

A practical framework community banks can use to govern, assess, and continuously manage AI risk.



Background

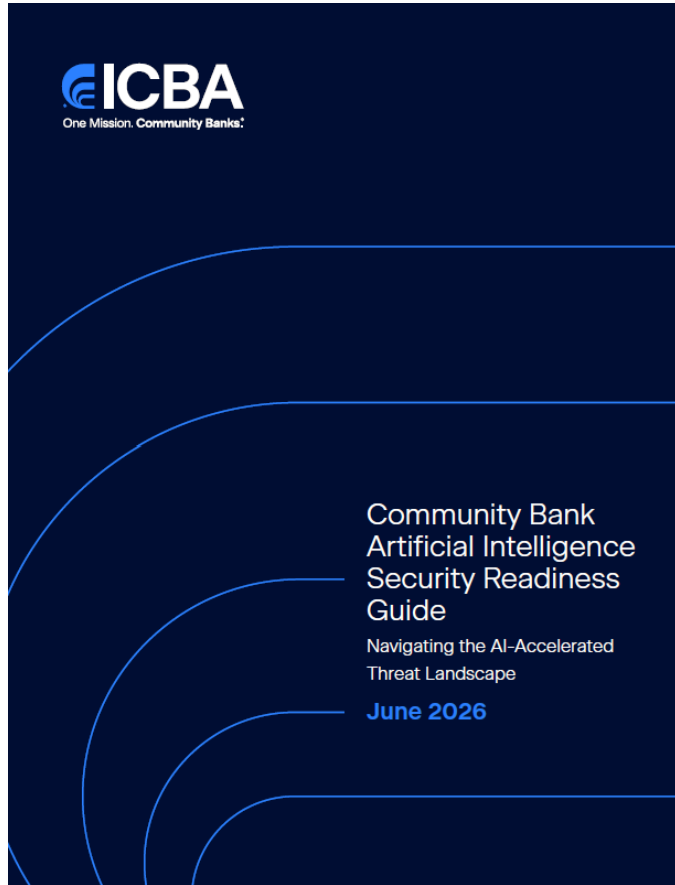
A voluntary, non-sector-specific National Institute for Standards and Technology (NIST) framework that helps organizations identify and manage AI risks across the AI lifecycle. It organizes AI risk work into four functions: Govern, Map, Measure, and Manage.

Key Takeaways

- Start with governance: assign ownership, approved uses, data rules, and escalation paths.
- Map your AI footprint: inventory use cases, vendors, data flows, and customer or decision impacts.
- Measure and manage risk: test outputs, monitor performance, and apply stronger controls to higher-risk uses.
- This is a key reference for the ICBA AI Security Readiness Guide, the CSBS AI Supervisory Framework, and the Financial Services AI Risk Management Framework.

Bottom Line: The AI RMF is not a regulation — it is a practical playbook for adopting AI in a safe, sound, and exam-ready way.

AI Task Force



A guide developed by community bankers for community bankers in partnership with ICBA
Released on June 2, 2026

What is in this ICBA guide?

30-pages:

- Quick Reference Guide for CEOs & BOD
- Overview on AI & Cybersecurity Landscape
- Briefing the Board on AI Security
- “Crown Jewel” Vendor Discovery
- Enhanced Vendor Due Diligence
- Incident Response Plan Updates & Tabletop Testing
- Addressing Implementation Challenges
- 90-Day Action Plan & Consolidated Checklist
- ICBA Resources

“This guide is going to help a lot of banks. I’ve already taken the checklist and imported into our project management tool.” - Luis Estrada, SVP at First Western Bank

Top 5 Priority Actions to Take Now - AI Security

1

Brief Your Board

Schedule a 20-minute AI security briefing within the next 30 days. Your CIO, CTO, or IT leads can facilitate.

2

Inventory Your AI

Before publishing any AI policy, find out what employees are already using. Discovery comes before governance.

3

Call Your Top 3 Vendors

Ask your core processor, online banking provider, and largest fintech partner: What AI is active in our environment right now?

4

Enroll in ICBA Tabletop Exercise – October 15 from 11:00am-2:00pm CT

ICBA offers federally partnered exercises with Treasury and CISA — typically satisfies examiner expectations at no additional cost to members.

5

Review Your Cyber Insurance

Confirm your policy covers incidents from third-party vendors and AI-assisted attacks. Many pre-2025 policies have gaps.

Consider Conducting an AI Risk Assessment

Use assessments to understand the risk your bank is accepting — and where governance, controls, training, and monitoring need to mature.

Choose the right assessment path

Self-Assessment

Best for banks with a very limited AI footprint, roughly 1 to 2 use cases, and clear internal ownership.

Consultants

Useful when use cases are expanding, governance is still forming, or the bank needs an independent gap assessment.

Insurance Providers

Can help connect AI-enabled cyber risk to coverage questions, underwriting expectations, and incident scenarios.

Law Firms

Helpful for higher-risk, consumer-facing, third-party, or decision-support use cases where legal and compliance implications matter.

What the assessment can produce

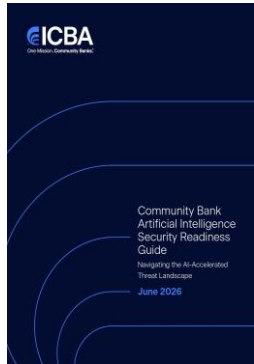
- A clear inventory of AI use cases, vendors, data flows, and business owners.
- A risk-tiered view of use cases based on consumer impact, data sensitivity, human oversight, and operational reliance.
- Practical next steps for policies, acceptable-use rules, vendor questions, staff training, testing, and monitoring.

IMPORTANT

No regulator currently prescribes a universal “AI risk score.” The assessment is not just a score but also a feedback loop that helps guide your bank’s AI adoption journey. The AI risk posture of your bank will change annually as AI evolves, and your use cases expand.

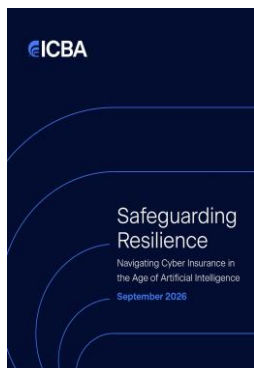
What's Coming From ICBA: More AI Readiness Support

Practical tools to help community banks prepare for AI adoption, cyber resilience, and emerging technology shifts.



Updated Community Bank AI Security Readiness Guide

Adds new sections on AI agents, bank-sourced AI due diligence questions, and emerging supervisory expectations.



Cyber Insurance White Paper

Helps banks navigate cyber insurance in the age of AI, including 30 questions to ask providers about coverage for AI-enabled incidents.



Supporting EO 14409 Implementation

Executive Order 14409: Promoting Advanced Artificial Intelligence Innovation and Security — additional support is in development to help community banks prepare for the next phase of advanced defensive AI capabilities.

State of AI in Community Banking

SURVEY & REPORT

The nation's first national survey focused on community bank AI adoption — translating early adoption stories into a practical benchmark for banks, policymakers, and technology partners.

~500

community banking institutions expected to be engaged

60 days

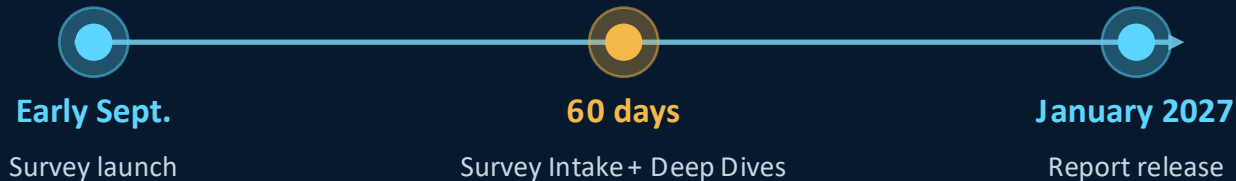
survey fielding window beginning in September 2026

15

banks already volunteered for adoption journey deep dives — more needed

Participation

Several ICBA members will receive the survey and are expected to complete it. Additionally, ICBA members are invited to volunteer for deep-dive adoption journey surveys to share more specifics about how they are leveraging AI.



ICBA ThinkTech Accelerator – AI Stack



HuLoop



Quilo™



posh



ATTUNE 

monit



Additional Resources & Literature

- The Conference of State Bank Supervisors – AI Supervisory Framework
<https://www.csbs.org/csbs-artificial-intelligence-supervisory-framework>
- ICBA Community Bank AI Security Readiness Guide
<https://www.icba.org/community-bank-artificial-intelligence-security-readiness>
- ICBA Cyber Insurance White Paper
<https://www.icba.org/cyber-and-data-security> (Mitigation Tab)
- Treasury and ICBA Tabletop Exercise Registration – October 15, 2026 | 11:00am-2:00pm CT
<https://www.icba.org/web/guest/p/treasury-and-icba-cyber-tabletop-exercise>
- NIST AI Risk Management Framework
<https://www.nist.gov/itl/ai-risk-management-framework>
- Cloud Security Alliance: Hugging Face Initial Post-Mortem
<https://cloudsecurityalliance.org/artifacts/hugging-face-ciso-post-mortem>
- NIST AI Agent Standards Initiative
<https://www.nist.gov/artificial-intelligence/ai-agent-standards-initiative>

Contact Information

Anjelica Dortch

Vice President, Operational Risk & Cybersecurity Policy

Anjelica.Dortch@icba.org

Washington, D.C.