JOINT TRADE ASSOCIATION LETTER ON AI-DRIVEN CYBERSECURITY RISK
&
A SECURE & AI-READY AMERICA ACTION PLAN

May 14, 2026

We, the undersigned trade associations, write to urge immediate Federal action to prepare for a new era of AI-enabled cybersecurity risk. Recent advances in artificial intelligence (AI) signal a structural shift in the cybersecurity environment facing the United States, particularly the private-sector owners and operators of critical infrastructure on which the Nation's security, economy, and daily life depend.

This is not a theoretical future challenge. Highly capable AI systems are accelerating vulnerability discovery, lowering the time and resources required to identify exploitable weaknesses, and increasing pressure on existing labor-intensive patching, incident response, disclosure, and risk management processes. Recent testing by cybersecurity companies confirms that frontier AI models can accomplish in weeks what previously required a full year of manual penetration testing, and adversaries can now weaponize new vulnerabilities within minutes of disclosure. Concerningly, these or similar systems will be available to adversary nations who might target the U.S. Government or private sector. The result is a rapidly changing threat environment in which longstanding assumptions, particularly about the speed of attack cycles, the scale of vulnerability discovery, and the integrity of the software supply chain no longer hold. On the other hand, in the medium- and long-term, these technologies should help create a more secure and resilient digital ecosystem that can continue to strengthen American businesses and improve the lives of citizens.

We believe this moment requires a whole-of-nation response commensurate with the size scale of the challenge. President Trump's *Cyber Strategy for America*, released in March 2026, makes clear that the Administration intends to streamline cyber regulations, modernize and secure Federal networks, strengthen the resilience of critical infrastructure, and adopt AI-powered cybersecurity solutions to defend Federal systems at scale. That strategic direction is well-suited to the threat environment now emerging. But today's rapidly evolving environment also requires a framework specifically tailored to AI-accelerated cyber risk, the secure deployment of agentic AI systems, and the resilience of the software and digital infrastructure on which the Nation depends. We must work together to translate pertinent elements of the Strategy into concrete action that prepares government and the private sector for the speed and scale of the AI era - particularly the implications of vulnerability discovery, observability, remediation, and risk-management lifecycles that are compressing in real time.

We welcome efforts by frontier AI model developers to raise awareness and promote collaboration through initiatives such as Anthropic's Project Glasswing. We encourage the U.S. government to foster voluntary structured and sustained engagement among frontier AI developers, policymakers, and critical infrastructure stakeholders to better identify emerging threats, test model capabilities, and strengthen national preparedness. Ongoing evaluation, red-teaming, and information sharing will be essential to staying ahead of rapidly evolving risks. At the same time, the U.S. government should work with AI companies to promote voluntary development, testing, and deployment practices that help protect society from the malicious use of advanced AI systems.

We stand ready to support this effort with technical expertise, operational insight, and participation in any public-private processes the Administration may convene. The following recommendations – each of which is aligned with President Trump's *Cyber Strategy for America* – will strengthen the Nation's cybersecurity and resilience and make America "AI-Ready."

1) **Adopt effective AI-driven cybersecurity and modernize security operations.** AI should be deployed as a force multiplier to enhance threat detection, incident response, and vulnerability management at scale. The same models that find and exploit vulnerabilities can be deployed in defense, but only if they are integrated into modern cybersecurity platforms supported by robust infrastructure, sensor networks, unified data lakes, and analytical tools that break down operational silos where critical signals are buried. To achieve this, the Administration should: reform procurement processes to embrace agile, outcomes-based approaches, that support the rapid adoption and iterative improvement of AI capabilities like machine learning and logging; direct federal agencies and critical infrastructure operators to rationalize fragmented security tooling, eliminating data silos and streamlining operations, and require public entities to conduct a frontier AI exposure analysis, deploy real-time, ML-based prevention and detection across all on-premises and cloud environments, and transform security operations into a near real-time function measured by Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

2) **Leverage existing resources and accelerate efforts to address targeted gaps.** The Administration should build on established cybersecurity guidance and industry best practices, rather than duplicating or fragmenting existing efforts. This includes supporting work to assess how current frameworks apply to emerging AI-related risks, identifying targeted gaps, and developing fit-for-purpose guidance to address those gaps along with accelerating the development and dissemination of resources to advance the secure deployment of AI generally, and agentic AI specifically, across the Federal Government and throughout the private sector. Over the past two years, the U.S. Department of the Treasury has worked closely with the financial services sector to examine AI's impact on cybersecurity and fraud and to launch several related workstreams. Those efforts recently produced papers on a financial services AI risk management framework, AI-enabled fraud, identity and authentication, explainability, nutrition labels, and AI lexicon. This work provides a strong model of public-private collaboration to develop practical solutions and policy recommendations, particularly in areas such as digital identity and authentication where government leadership remains important.

3) **Reestablish cross-sector public-private coordination to help facilitate AI cyber readiness and response.** The administration should expand public-private collaboration, and specifically, the Administration should leverage and modernize the Critical Infrastructure Partnership Advisory Council (CIPAC) framework to ensure regular engagement among departments and agencies, sector risk management agencies (SRMAs), critical infrastructure owners and operators, technology providers, cybersecurity firms, and relevant trade associations.

4) **Conduct a national risk assessment.** The Administration should conduct a comprehensive assessment of AI-related security risks and opportunities at the national level, including recommendations, with particular focus on AI-enabled vulnerability discovery, observability, exploitation, risk-management and remediation, as well as agentic AI cyber capabilities.

5) **Update cybersecurity risk and resilience management plans.** The Administration should direct departments and agencies to modernize their cybersecurity and resilience risk management plans in light of technological developments in AI and quantum computing, including by prioritizing the transition to Zero Trust architectures, immutable and isolated backup copies of mission-essential data, and post-quantum cryptography (PQC) to address future risks to encryption. The Administration should also reconsider key elements such as approaches to governing cybersecurity activities and specifically the adoption of AI for cybersecurity and resilience purposes and preparation for the misuse of AI by malicious actors.

6) **Modernize coordinated vulnerability disclosure and the CVE ecosystem.** The Administration should invest in the CVE ecosystem so it can operate effectively in a global environment and meet AI-accelerated vulnerability discovery and exploitation, as well as the increase in volume.

7) **Refocus the Cybersecurity and Infrastructure Security Agency on its core mission.** The Administration should prioritize CISA activities that directly advance its core mission of protecting the federal civilian government networks; sharing information with private-sector partners; and supporting critical infrastructure owners and operators – all of which are critical to addressing the unique challenges posed by the speed and scale of advanced AI systems.

8) **Advance an AI-ready America workforce strategy.** The Administration should work with industry to produce and execute a workforce strategy that strongly matches Americans to jobs of the future, strengthens the Nation's cybersecurity talent pipeline, expands AI literacy, and builds the surge capacity needed to respond to AI-accelerated cyber threats.

9) **Streamline and eliminate unnecessary regulations, beginning with cyber incident reporting.** The Administration should move quickly to rationalize cyber incident reporting requirements before AI-accelerated threats and higher-volume vulnerability activity place unsustainable pressure on already strained security teams and ensure regulated entities and their third-party service providers are not forced to satisfy overlapping timelines, definitions, and reporting formats across multiple Federal regimes, including revisiting the Securities and Exchange Commission's regulation on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

10) **Work with Congress to take steps necessary to prepare for an AI world.** The Administration should prioritize reauthorizing the Cybersecurity Information Sharing Act of 2015 and updating M-21-31: *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. These frameworks help private sector organizations share and continuously monitor cybersecurity threats that help protect the government, businesses, and the American people. In addition, the administration should fill key government roles like the Ambassador for Cyberspace and Digital Policy, and the Directors of the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology.

11) **Expand American leadership and cooperation with international partners.** The Administration should strengthen American leadership and deepen coordination with like-

minded partners to advance the development and adoption of AI systems, including AI agents, and drive alignment in critical areas such as vulnerability disclosure, technical standards, and cross-border cyber incident response and reporting.

12) **Promote structured public-private collaboration to test advanced AI models for security risk.** The Administration should encourage sustained collaboration among frontier AI developers, relevant Federal agencies, and critical infrastructure stakeholders to support the testing, evaluation, and red-teaming of advanced AI models for cybersecurity, fraud, resilience, and broader national security risks. As model capabilities evolve rapidly, ongoing and trusted collaboration built on open standards will be essential to ensure transparency and interoperability. This initiative should help identify risks to improve shared understanding of model behavior in real-world environments, and inform practical safeguards, response protocols, and policy development.

Each of the preceding recommendations has accompanying specific actions for government offices and agencies, including the Office of the National Cyber Director (ONCD), Office of Management and Budget (OMB), Cybersecurity and Infrastructure Security Agency (CISA), National Institute for Standards and Technology (NIST), the U.S. Department of State and others, which we look forward to discussing as we partner to achieve our shared goal of a more secure and resilient digital ecosystem.

Thank you for your consideration of this letter and action plan.

Respectfully Submitted,

Alliance for Chemical Distribution
American Fintech Council
Business Software Alliance
Cybersecurity Coalition
Cyber Threat Alliance
Electronic Transactions Association
Healthcare Leadership Council
Independent Community Bankers of America
National Electrical Manufacturers Association
TechNet