Leading American Trade Associations Urge Federal Action to Address AI-Enabled Cyber Risk

Press Release: Washington, D.C. (May 14, 2026)—A cross-sector of trade associations representing energy, electricity manufacturers, technology, financial services, healthcare, chemical distribution, and other critical infrastructure sectors today urged the administration to take coordinated action to address emerging AI-enabled cyber risk. In a letter to the administration, the groups highlighted the deeply interconnected nature of sector-wide risk and put forward a set of recommendations to strengthen the resilience and security of America's critical infrastructure sectors.

"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," the group wrote. "We stand ready to support this effort with technical expertise, operational insight, and participation in any public-private processes the Administration may convene."

While AI advancements will lead to a more secure and resilient digital ecosystem long-term, ongoing collaboration will be essential to identify emerging threats, test model capabilities, and strengthen national preparedness consistent with the goals outlined in President Trump's Cyber Strategy for America plan.

"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," the groups wrote.

In its letter, the group called for:

- **Adoption of AI-driven cybersecurity capabilities and modernization of security operations.** Deploy AI as a force multiplier for detection, response, and vulnerability management—supported by modern platforms and rationalized tooling that breaks down data silos for near-real-time operations.
- **Enhanced public-private coordination and information sharing**. Strengthen sustained, structured engagement across government, sector risk management agencies, critical infrastructure stakeholders, and providers—leveraging and modernizing existing coordination mechanisms to support AI cyber readiness, response, and timely information sharing.
- **Modernization of vulnerability disclosure and incident response frameworks**. Invest in the CVE ecosystem for AI-accelerated volume while updating federal investigative and remediation frameworks to keep pace with compressed attack cycles.
- **Strengthened cybersecurity and AI workforce development**. Advance an AI-ready workforce strategy that grows the cybersecurity talent pipeline, expands AI literacy,

and builds surge capacity so organizations can respond to faster, higher-tempo AI-enabled threats.

- **Streamlining duplicative cyber regulations and reporting requirements**. Rationalize cyber incident reporting to reduce overlapping timelines, definitions, and formats across federal regimes to limit avoidable strain on security teams.
- **Practical frameworks for AI risk management, resilience, and secure deployment**. Build on established cybersecurity guidance to address targeted AI gaps and modernize cyber/resilience plans with priorities including Zero Trust, immutable and isolated backups, post-quantum cryptography readiness, and preparation for malicious use.
- **Structured collaboration among government, critical infrastructure sectors, and frontier AI developers to test and evaluate advanced AI systems**. Support sustained testing and red-teaming, trusted information sharing, and structured collaboration to inform practical safeguards, response protocols, and responsible development and deployment practices.

The group looks forward to partnering with policymakers to build a more secure and resilient digital future for all Americans.

Co-signatories include:
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