CTA™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

March 9, 2026

via www.regulations.gov

Center for AI Standards and Innovation
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Re: Request for Information Regarding Security Considerations for Artificial Intelligence Agents (NIST-2025-0035)

The Consumer Technology Association® ("CTA") submits these comments in response to the Center for AI Standards and Innovation at the National Institute of Standards and Technology's ("NIST") request for information ("RFI") on measuring and improving the security of artificial intelligence ("AI") agent systems. As North America's largest technology trade association, CTA is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs.

CTA member companies lead the development and deployment of AI systems that improve productivity, accelerate research and development, and deliver new solutions across health care, energy, agriculture, mobility, and other sectors. AI agent systems will play an increasingly important role in this innovation ecosystem. By enabling more efficient automation, decision support, and task execution, AI agents have the potential to drive substantial economic value. One estimate suggests AI agent systems could generate between $450 billion and $650 billion in additional annual revenue by 2030 while reducing operating costs by 30 to 50 percent.

CTA supports NIST's continued leadership in developing voluntary, consensus-driven frameworks that strengthen AI security while enabling innovation. As AI agent systems rapidly evolve, NIST should build on existing cybersecurity and AI risk management foundations, particularly the NIST Artificial Intelligence Risk Management Framework ("AI RMF"), and continue collaborating closely with industry to develop flexible and scalable approaches to AI security.

CTA has long supported industry-driven technical standards that improve transparency, trust, and security in AI systems. CTA is an American National Standards Institute ("ANSI") accredited standards development organization, and our standards have provided industry guidance since 1924 with more than 1100 active participants.

CTA has led the way on industry-driven technical standards governing AI use and development, including:

- ANSI/CTA-2090: The Use of Artificial Intelligence in Health Care: Trustworthiness
- ANSI/CTA-2096: Guidelines for Developing Trustworthy Artificial Intelligence Systems
- CTA-5203: Cybersecurity Threats and Security Controls for Machine Learning Based Systems
- ANSI/CTA-2107-A: The Use of Artificial Intelligence in Health Care: Managing, Characterizing, and Safeguarding Data
- ANSI/CTA-2135: Performance Verification and Validation for Predictive Health AI Solutions

Most recently, CTA adopted a standard, CTA-2114: Mitigating Cybersecurity Threats in ML-Based Systems, establishing a framework for mitigating security threats unique to machine learning-related products.[1] The standard identifies security threats applicable to AI agent systems, including document injection and poisoning, prompt injection via retrieved content, and untrusted tool outputs.[2] It also recommends controls to address these threats including training data sanitization, provenance-based poison detection, model validation, data segregation, access controls, and other mechanisms that strengthen data integrity and system reliability.[3] Importantly, the CTA-2114 standard is not prescriptive. Instead, it provides an evolvable framework that organizations can adapt to their specific systems, risk environments, and operational needs.[4]

NIST should continue working with industry to create consensus-based frameworks for AI agent system security that address the rapidly changing risk landscape around AI agents. Drawing on the industry's breadth of technical expertise and experience, NIST and industry can work together to create flexible standards suitable for organizations of all sizes and new innovations and risks. A flexible approach will facilitate experimentation and iterative development appropriate to the nascent stage of AI agent system development.

NIST should build on the strong foundation of the AI RMF, which provides an evolvable framework that organizations can adapt to their specific systems, risk environments, and operational needs. Although AI agent systems introduce certain novel risks, many security considerations associated with these systems can be addressed through existing cybersecurity and AI risk management practices reflected in the AI RMF. NIST should therefore ensure that future guidance addressing AI agent systems aligns with the AI RMF and reinforces its core principles.

[1] The standard defines a machine learning system as a "subset of AI where a machine adapts its behavior based on patterns and insights derived from past data, akin to the learning process of complex systems." CTA-2114: Mitigating Cybersecurity Threats in ML-Based Systems at 1.

[2] *Id*. at 46–47.

[3] *Id*. at 30, 32.

[4] *Id*. at 1.

One of the AI RMF's key features is that it is non-prescriptive. The AI RMF allows developers and deployers the flexibility to scale their risk management activities appropriately. NIST should continue to avoid prescriptive, technical approaches when considering AI agent system security. Specifically, any approach should be flexible: risk-based, scalable, and iterative.

The RFI describes AI agent systems as systems that combine generative AI models with software scaffolding that enables the model to plan and execute actions that affect real-world systems or environments. These systems support a wide range of applications, including customer service automation, fraud detection, and clinical decision support. Because these use cases vary widely in potential impact and risk, security frameworks should remain risk-based and adaptable rather than prescriptive.

At this early stage of AI agent system development, NIST should also emphasize iterative approaches to guidance and framework development. AI technologies continue to evolve rapidly, and flexible guidance will allow organizations to adapt security practices as the technology matures and new risks emerge.

CTA urges NIST to continue collaborating with industry in developing approaches to AI agent system security. Industry has deep technical expertise and experience implementing cybersecurity controls and frameworks for new technologies. Leveraging this expertise will help ensure that emerging AI security frameworks remain practical, interoperable, and responsive to real-world deployment challenges.

CTA appreciates NIST's ongoing collaboration with industry to create voluntary, flexible AI frameworks that promote both trustworthiness and innovation. By building on the AI RMF and maintaining a flexible, risk-based approach, NIST can strengthen trust in AI systems while preserving the agility needed to innovate. This approach will support rapid development and deployment of AI technologies and reinforce American leadership in artificial intelligence.

Sincerely,

CONSUMER TECHNOLOGY ASSOCIATION

/s/
J. David Grossman
Vice President, Policy & Regulatory Affairs

/s/
Kerri Haresign
Senior Director, Technology & Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651