Crowell

NIST Releases Draft Framework for AI Cybersecurity, Solicits Public Comment: What Organizations Using or Deploying AI Should Know

What You Need to Know

Key takeaway #1

This is an “Initial Preliminary Draft” of the Cyber AI Profile. The Draft is intended to convey current thinking regarding the direction of AI governance and the authors seek feedback to inform future iterations. The deadline for public comments is January 30, 2026.

Key takeaway #2

The Cyber AI Profile does not replace any existing cybersecurity or AI governance frameworks; rather, it layers AI-specific priorities and considerations onto the CSF 2.0.

Key takeaway #3

The Cyber AI Profile has the potential to become a de facto benchmark for regulators, federal agencies, and plaintiffs assessing cybersecurity diligence involving AI.

Client Alert | 4 min read | 01.13.26

The National Institute of Standards and Technology (“NIST”) recently released draft guidelines for applying NIST’s Cybersecurity Framework to organizations adopting artificial intelligence. NIST requests **public comments** on its “Initial Preliminary Draft” **Cybersecurity Framework Profile for Artificial Intelligence** (the “Cyber AI Profile”) by midnight on January 30, 2026.

Although nonbinding, the Cyber AI Profile is significant because it provides organizations with guidelines for managing cybersecurity risks related to AI systems. It represents NIST’s first comprehensive attempt to integrate AI-specific risks and opportunities directly into the NIST **Cybersecurity Framework 2.0** (“CSF”), the Institute’s widely-used standard for managing cybersecurity risks. Organizations that develop, deploy, procure, or rely on AI systems should view the Cyber AI Profile as an early sign of how regulators, auditors, plaintiffs, and counterparties may evaluate “reasonable” cybersecurity and governance practices for AI-enabled systems.

The Cyber AI Profile addresses three areas where the intersection of AI and cybersecurity will be particularly impactful:

- Securing AI System Components, which focuses on identifying cybersecurity challenges when integrating AI into organizational ecosystems and infrastructure;
- Conducting AI-Enabled Cyber Defense, which focuses on identifying opportunities to use AI to enhance cybersecurity processes and activities; and
- Thwarting AI-Enabled Cyber Attacks, which focuses on building resilience to protect against new AI-enabled threat vectors.

Key Takeaways

- This is an "Initial Preliminary Draft" of the Cyber AI Profile. The Draft is intended to convey current thinking regarding the direction of AI governance and the authors seek feedback to inform future iterations. The deadline for public comments is January 30, 2026.
- The Cyber AI Profile does not replace any existing cybersecurity or AI governance frameworks; rather, it layers AI-specific priorities and considerations onto the CSF 2.0.
- The Cyber AI Profile has the potential to become a de facto benchmark for regulators, federal agencies, and plaintiffs assessing cybersecurity diligence involving AI.

What Is the Cyber AI Profile?

The Cyber AI Profile is a NIST Cybersecurity Framework Community Profile designed to help organizations prioritize cybersecurity outcomes in the context of AI systems. Importantly, NIST deliberately avoids narrowly defining "AI," instead using the term "AI systems" to refer to any system that is using AI capabilities, whether they are stand-alone AI systems or applications, infrastructure, and organizations that incorporate AI. Thus, the Cyber AI Profile is intended to apply broadly across large language models ("LLMs"), generative AI, predictive analytics, recommendation engines, agentic systems, and hybrid approaches.

In general, the Cyber AI Profile:

- Uses the CSF 2.0 Functions, Categories, and Subcategories (Govern, Identify, Protect, Detect, Respond, Recover), which group together similar cybersecurity measures that organization can implement;
- Adds AI-specific considerations and proposed priorities for each Subcategory, such as incorporating AI audits to address AI-specific needs (like explainability); and
- Recognizes that organizations may be at very different stages of AI adoption—from limited machine learning tools to fully agentic or generative AI deployments.

Application and Related Initiatives

The Cyber AI Profile is intended for a broad array of organizations. These include those developing or using AI technologies, whether they are stand-alone AI systems or AI-enabled capabilities that are integrated into other systems. They also include those that would like to understand and capitalize on the cybersecurity capabilities that AI can provide or to better understand and defend against AI-enabled cyber-attacks.

To complement the Cyber AI Profile and support the adoption of its separate AI Risk Management Framework, NIST is developing a series of **Control Overlays for Securing AI Systems (COSAiS)** using the **NIST Special Publication (SP) 800-53 controls**. This effort should allow organizations to tailor their baseline security measures—or "controls"—to their specific context and needs. COSAiS plans to provide additional implementation guidelines and to assist AI users and developers manage their unique risks across different use cases, such as adapting and using generative AI, using and fine-tuning predictive AI, and using agentic AI. Simultaneously, NIST has announced a **Request for Information** on how to measure and improve the secure development and deployment of agentic AI systems, laying the groundwork for more in-depth guidance to come.

Separately, the Fiscal Year 2026 National Defense Authorization Act has **directed** the Pentagon to create and implement a security assessment framework for the AI technologies that it procures. Given the frequency with which the Pentagon has mandated compliance with NIST cybersecurity standards, it will likely consider NIST's burgeoning list of AI guidance, including the developing Cyber AI Profile, when crafting this new AI security requirement.

Conclusion

NIST's Cyber AI Profile signals a clear message: AI is a cybersecurity governance issue. Organizations that wait for binding regulation before adapting their programs may find themselves behind emerging expectations.

Crowell & Moring will continue to monitor developments, including the finalization of the Cyber AI Profile and NIST's Control Overlays for Securing AI Systems. For questions about how this draft may affect your AI deployments, cybersecurity posture, regulatory exposure, or contractual obligations, please contact our team.

Contacts

Matthew F. Ferraro
Partner
Washington, D.C. D | +1.202.624.2610
mferraro@crowell.com

Kate M. Growley
Partner, Crowell Global Advisors Senior Director
Washington, D.C. D | +1.202.624.2698
Washington, D.C. (CGA) D | +1 202.624.2500
kgrowley@crowell.com

Michael G. Gruden
Partner
Washington, D.C. D | +1.202.624.2545
mgruden@crowell.com

Jacob Canter
Counsel
He/Him/His

San Francisco D | +1.415.365.7210
jcanter@crowell.com