GOODWIN

JANUARY 28, 2026

AI Risk Meets Cyber Governance: NIST's Draft Cyber AI Profile

Kaitlin Betancourt, Peter M. Marta, L. Judson Welle, Corey Berman

On December 16, 2025, the National Institute of Standards and Technology ("NIST"), a non-regulatory federal agency within the U.S. Department of Commerce that promotes innovation through technical standards setting, released a preliminary draft of its forthcoming Cyber AI Profile. The Cyber AI Profile aims to help organizations bolster artificial intelligence ("AI") governance leveraging NIST's Cybersecurity Framework 2.0 (the "CSF") as a guide to the cybersecurity of AI systems and the use of AI to support cybersecurity. Like the CSF, the Cyber AI Profile is voluntary for most organizations; however, organizations that align their risk management practices to these resources tend to be viewed by customers, investors, and regulators as more secure, resilient, and responsible.

The Cyber AI Profile identifies three overarching AI focus areas, or themes, related to organizational AI governance:

- **Securing AI System Components ("Secure"):** Companies are encouraged to supplement existing risk management approaches to account for the new challenges posed by integration of AI systems, including AI supply chains, infrastructure, and other dependencies.
- **Conducting AI-Enabled Cyber Defense ("Defend"):** Companies should work to leverage AI to strengthen cybersecurity defenses, whether by using AI to manage an increased volume of threat intelligence, integrating agentic AI to automate collaborative incident response tasks, or increasing efficiencies across IT operations and help desks.
- **Thwarting AI-Enabled Cyber Attacks ("Thwart"):** Companies must prepare for how adversarial use of AI increases threat actor sophistication, expands potential attack surfaces, and introduces new risks, including deepfake attacks targeting organization personnel, generative AI-enabled fraud, and autonomous agent-driven vulnerability exploitation.

Rather than prescribing particular requirements, the Cyber AI Profile consists of recommended considerations for implementing AI governance within the CSF. The Cyber AI Profile maps each of the AI focus areas onto the six core functions of the CSF (Govern, Identify, Protect, Detect, Respond, and Recover) and provides priorities and recommended considerations to help companies achieve the CSF's desired outcomes. For example, under the CSF's Govern function, the Cyber AI Profile recommends prioritizing "Secure" AI by ensuring that relevant teams understand the business outcomes that rely on AI and can

effectively assess AI decisions and respond when AI systems make errors.

The Cyber AI Profile is part of a growing trend of guidance that fuses AI governance and cybersecurity risk governance. Both federal and state regulators have highlighted the correlation. Additional background and insights on the intersection between AI and cybersecurity can be found here.

Rather than introducing an entirely new framework for managing the cybersecurity risks posed by AI, the Cyber AI Profile encourages organizations to consider AI governance a logical extension of existing cybersecurity approaches and provides a familiar and common language for managing these risks. The Cyber AI Profile also provides suggested prioritizations to help guide companies through the most important outcomes for achieving the AI focus areas. For example, a subcategory ranked in the Cyber AI Profile as priority 1 indicates a particularly important activity for mitigating risk at the intersection of cyber and AI.

The Cyber AI Profile is broadly applicable but could prove particularly useful for organizations seeking to demonstrate cybersecurity maturity, including as required by customers and investors, or under the following regulatory frameworks:

- **Covered Entities Regulated by the New York State Department of Financial Services ("NYDFS"):** Under guidance in connection with its cybersecurity regulation, 23 NYCRR Part 500 ("Part 500"), NYDFS has similarly highlighted the interconnected relationship of cybersecurity and AI and outlined considerations for regulated insurance and financial services companies. On October 16, 2024, NYDFS recommended a series of controls to mitigate AI risk under its existing Part 500 framework. In its industry letter, NYDFS specifically addressed the changing nature of cyber risk in light of AI and noted that, while its guidance would stop short of formalizing new AI-focused Part 500 requirements, businesses should proceed to incorporate AI's cybersecurity risks into the Part 500 framework.

  From the increased viability of social engineering-based cyberattacks to lowered barriers for threat actors to access business systems, NYDFS now encourages covered entities to identify material updates to cybersecurity risk assessments in light of AI-related risk. Covered entities should take into account AI when assessing third-party vendor management controls, strengthening multifactor authentication processes, enhancing cybersecurity training for employees, and implementing robust system monitoring.

  NYDFS covered entities may have previously utilized tools such as the Cyber Risk Institute ("CRI") Profile, which provided a similar mapping to frameworks such as the CSF 2.0 and Part 500. With the rollout of NIST's Cyber AI Profile, covered entities will have an additional tool providing a shared vocabulary for incorporating AI into cybersecurity risk frameworks in alignment with Part 500's requirements.

- **Public Companies Regulated by the U.S. Securities and Exchange Commission ("SEC"):** Public companies will likewise benefit from a review of the Cyber AI Profile. Although the SEC's Investor Advisory Committee ("IAC") in December 2025 formally recommended that the SEC establish more prescriptive AI disclosure frameworks for issuers, SEC Chairman Paul Atkins registered his desire for the SEC to "resist the temptation" to introduce entirely new rules "for every 'new thing' that affects a business," instead describing a preference for public companies to use existing rules to advise investors of the impacts of AI on financial results, risk factors, and business models.

In the absence of defined, AI-specific disclosure guidance, public companies may increasingly rely on tools such as the Cyber AI Profile to contextualize AI-powered risk as part of broader cybersecurity risk management and governance programs, including in connection with Form 10 K and other public disclosures.

- **Registered Investment Advisors Regulated by the SEC:** Registered investment advisers and other covered institutions subject to SEC oversight may also wish to consider the Cyber AI Profile as they take steps to address recent amendments to Regulation S-P, the SEC's rule governing the safeguard and proper disposal of customer information.

  Regulation S-P traditionally required written policies and procedures to protect customer records and was recently amended to impose additional cybersecurity-focused obligations governing incident response procedures, customer notification requirements, service provider oversight, and other obligations. Larger covered institutions were required to be in compliance with the amendments by December 3, 2025, and other covered institutions will be subject to the amendments as of June 3, 2026. The confluence of AI and cybersecurity was among the priorities specifically noted in the SEC's recently published examination priorities and FINRA's Annual Regulatory Oversight Report. In preparation for the upcoming examination season, covered entities should ensure that they maintain comprehensive AI risk governance processes that appropriately treat AI as one component of their bigger-picture, integrated cybersecurity risk framework.

Next Steps

The comment period for the draft Cyber AI Profile remains open through January 30, 2026. The current draft is expected to evolve following industry and stakeholder feedback. Organizations should continue to monitor NIST's progress toward publication of a final Cyber AI Profile.

In the interim, businesses seeking to align cybersecurity and AI risk management, especially those whose cybersecurity, data protection, and AI risk management activities are closely scrutinized, should consider the Cyber AI Profile as a tool for evaluating and refining existing programs. Organizations already familiar with the CSF Profiles may wish to begin integrating elements of the Cyber AI Profile into their cybersecurity risk assessments. Others may look to the Cyber AI Profile for guidance in prioritizing AI-related cyber risks, validating existing risk assessments, and informing decisions around the allocation of financial resources, time, and personnel in the months ahead.

CONTACTS

Kaitlin Betancourt
Partner
Data, Privacy & Cybersecurity
kbetancourt@goodwinlaw.com

Peter M. Marta
Partner
Complex Litigation & Dispute Resolution
petermarta@goodwinlaw.com

L. Judson Welle
Partner
Data, Privacy & Cybersecurity
jwelle@goodwinlaw.com

Corey Berman
Associate
coreyberman@goodwinlaw.com