WILLKIE

CLIENT ALERT

NYDFS Issues Two Industry Letters Addressing Heightened Cybersecurity Risks from Frontier AI Models and Guidance for Heightened Threat Environments

May 29, 2026

AUTHORS

Daniel K. Alvarez | Matthew J. Gaul | Laura E. Jehl | Amelia Putnam
Shlomo Potesky | Lorna Strachan

On May 21, 2026, the New York Department of Financial Services ("NYDFS") issued two related Industry Letters addressing cybersecurity risks facing regulated entities: (1) an Advisory on the heightened cybersecurity risks associated with certain frontier artificial intelligence models[1] (the "AI Advisory"), and (2) guidance on measures regulated entities should consider in a heightened cybersecurity threat environment[2] (the "Heightened Threat Guidance Letter") (together, the "Industry Letters"). While neither Industry Letter imposes new legal requirements, both signal that NYDFS expects covered entities to take concrete steps to adjust to the changing threat landscape,

[1] Industry Letter, N.Y. Dep't of Fin. Servs., Heightened Cybersecurity Risks Associated with Frontier AI Models, May 21, 2026, https://www.dfs.ny.gov/industry-guidance/industry-letters/20260521-heightened-cybersecurity-risks-assoc-with-frontier-ai-models ("Frontier Models Letter").

[2] Industry Letter, N.Y. Dep't of Fin. Servs., Guidance on Measures Regulated Entities Should Consider in a Heightened Cybersecurity Threat Environment, May 21, 2026, https://www.dfs.ny.gov/industry-guidance/industry-letters/20260521-guidance-on-measures-reg-entities-should-consider-in-a-hcte ("Heightened Threat Guidance Letter").

particularly in light of the broader availability of advanced AI capabilities. Regulated entities should carefully assess whether their current cybersecurity programs adequately address the risks identified in the Industry Letters.

The AI Advisory: Heightened Cybersecurity Risks Associated with Frontier AI Models

The AI Advisory warns of heightened cybersecurity risks associated with "Frontier AI Models," which NYDFS explains can "amplify the potency, scale, and speed of identifying vulnerabilities and exploits in information systems."[3] The AI Advisory seems likely to have been prompted by Anthropic's announcement of Mythos, which is an advanced AI model that has demonstrated unprecedented capabilities in identifying and exploiting software vulnerabilities—including, according to reports, finding thousands of previously unknown "zero-day" flaws in every major operating system and web browser.[4]

In the AI Advisory, NYDFS urges regulated entities to improve their security posture in preparation for the broader availability of Frontier AI Models that can readily be used by threat actors to undermine existing security efforts, emphasizing that the best preparation is "a robust cybersecurity program that includes timely and comprehensive vulnerability identification and remediation."[5] The AI Advisory directs regulated entities to consider various cybersecurity measures outlined in the Heightened Threat Guidance Letter, such as expedited vulnerability management, coordination with third-party service providers on vulnerability management and review of threat intelligence, and strengthened testing of AI-generated code prior to production deployment.

The AI Advisory notes that this is "not an exhaustive list" and that entities should "consider taking whatever steps are necessary" to manage their unique cybersecurity risks in light of rapid developments in Frontier AI Models.

The Heightened Threat Guidance Letter: Measures for Elevated Cybersecurity Environments

The Heightened Threat Guidance Letter provides a broader framework of recommended practices for "heightened threat environments" when cybersecurity risks are "significantly elevated and therefore have a high likelihood of impacting Information Systems, Nonpublic Information or operations."[6] NYDFS expressly identifies the release of Frontier AI Models as a technological development that may trigger a heightened threat environment.

The Heightened Threat Guidance Letter organizes its non-exhaustive list of best practices into three categories:

> **Category 1 – Measures to Reduce the Attack Surface:** This category describes actions a regulated entity can take to minimize the number of potential entry points that an attacker could exploit to compromise a system or network. Such measures include expedited vulnerability remediation for internet-facing systems, disabling unnecessary ports and protocols, restricting multifactor authentication ("MFA") enrollment changes and employing phishing-resistant MFA, among other measures.

---

3 *See* Frontier Models Letter.

4 *See Project Glasswing*, ANTHROPIC, https://www.anthropic.com/glasswing.

5 *See* Frontier Models Letter.

6 *See* Heightened Threat Guidance Letter.

Category 2 – Measures to Improve Threat Detection and Readiness: This category outlines strategies a regulated entity can put in place to better identify cybersecurity threats and to ensure it is prepared to respond effectively when those threats materialize. Examples of these measures include confirming that intrusion detection controls are current and deployed, capturing log and alerting data with prompt action on anomalies, and reviewing threat intelligence and indicators of compromise.

Category 3 – Measures to Improve Resilience and Response: The final category details measures that can help a regulated entity prepare and test its cybersecurity responses. These measures include testing backup integrity and recovery time objectives, and reviewing and testing incident response and business continuity plans.

The Heightened Threat Guidance Letter emphasizes that whether a regulated entity should adopt such practices "depends on the unique circumstances and operations of an organization" and its specific threat profile, systems, and supply chain dependencies.

What Regulated Entities Should Do Now

In light of these Industry Letters, regulated entities should consider the following steps:

1. **Update Risk Assessments to Address Frontier AI Model Threats.** Risk assessments should be updated to include an assessment of how Frontier AI Models may be used to identify and exploit vulnerabilities in the regulated entity's systems.

2. **Accelerate Vulnerability Management Programs.** Regulated entities should evaluate whether current vulnerability management timelines are adequate, given the speed at which Frontier AI Models can identify exploitable weaknesses, and should consider reducing remediation windows where necessary.

3. **Assess and Strengthen Third-Party Risk Management.** Regulated entities should initiate discussions with critical third-party service providers regarding *their* preparedness for AI-enabled threats. Regulated entities should also ensure that contractual protections bind those service providers to implement reasonable information security controls and to provide the regulated entity with timely notification of cybersecurity events.

4. **Review and Harden Secure Programming Practices.** Regulated entities should implement additional testing, validation, and human oversight for AI-generated code before deployment in production environments, particularly to the extent such oversight is not already in place.

5. **Enhance Monitoring, Logging, and Alerting Capabilities.** Regulated entities should consider whether additional logging, more granular alerting rules, or expanded behavioral analytics are warranted.

6. **Test Incident Response and Business Continuity Plans.** Regulated entities should review and test operational resilience procedures with a specific focus on AI-enabled threat scenarios.

7. **Brief Executives.** Regulated entities should ensure that their Boards and senior officers are informed of the Industry Letters, including NYDFS's expectations regarding Frontier AI Model risks and the challenges those AI models pose for cybersecurity programs.

8. **Reassess Legacy and End-of-Life Systems.** Regulated entities should consider advancing plans for end-of-life or legacy information systems that may be particularly vulnerable to exploitation by AI-enabled threat actors.

Conclusion

The Industry Letters underscore the NYDFS's expectations that regulated entities take a proactive posture toward AI-related cybersecurity risks, and the Industry Letters signal that regulated entities should expect heightened scrutiny in this area. Regulated entities should promptly review and update their cybersecurity programs to account for threats posed by Frontier AI Models. Regulated entities should treat the Industry Letters as an urgent call to action—particularly given NYDFS's track record of pursuing enforcement actions against entities that fail to keep pace with its cybersecurity expectations.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	**Matthew J. Gaul**	**Laura E. Jehl**	**Amelia Putnam**
202 303 1125 dalvarez@willkie.com	212 728 8261 mgaul@willkie.com	202 303 1056 ljehl@willkie.com	202 303 1089 aputnam@willkie.com
Shlomo Potesky	**Lorna Strachan**		
212 728 3232 spotesky@willkie.com	202 303 1264 lstrachan@willkie.com		

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HAMBURG HOUSTON LONDON LOS ANGELES
MILAN MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON