GT GreenbergTraurig

**Alert | Financial Regulatory & Compliance/ Data Privacy & Cybersecurity**

June 2026

# NYDFS Issues Dual Guidance on Heightened Cybersecurity Threats, Frontier AI Risks

**Go-To Guide:**

- On May 21, 2026, the New York Department of Financial Services (NYDFS) published two companion industry letters: a guidance on measures regulated entities should consider in a heightened cybersecurity threat environment, and an advisory on the cybersecurity risks posed by frontier AI models.
- The **Heightened Threat Environment Guidance** catalogs specific measures across three categories: reducing the attack surface, improving threat detection and readiness, and strengthening resilience and response.
- The **Frontier AI Advisory** directs CISOs to particular sections of the Heightened Threat Environment Guidance and layers on AI-specific recommendations for vulnerability management, secure coding, and third-party coordination.
- Neither publication creates new legal requirements under 23 NYCRR Part 500. Both articulate DFS's expectations for how regulated entities should calibrate their existing cybersecurity programs when threat conditions escalate. Still, both publications preview examination expectations.

On May 21, 2026, NYDFS published two related industry letters addressing cybersecurity preparedness for DFS-regulated financial institutions, insurers, and money transmitters. The first, titled Guidance on Measures Regulated Entities Should Consider in a Heightened Cybersecurity Threat Environment (the Guidance), provides a structured menu of defensive measures entities should consider when cybersecurity risks become significantly elevated. The second, titled Heightened Cybersecurity Risks Associated with Frontier AI Models (the Advisory), warns that certain AI models capable of identifying vulnerabilities and exploits at unprecedented speed and scale will soon become more widely available, and directs entities to prepare now. The two documents are designed to work together: the Advisory identifies the threat, and the Guidance provides recommendations on how to respond.

Neither publication creates binding requirements. Both documents state explicitly that they do not alter the obligations under Part 500. The Guidance frames its recommendations as measures entities "should consider" adopting based on their "unique circumstances and operations." The Advisory states it is "intended to inform Regulated Entities' risk management and compliance efforts."

That said, NYDFS has a well-established pattern of publishing non-binding guidance that later becomes the benchmark in examinations and enforcement. NYDFS may evaluate whether an entity considered these measures, documented its reasoning, and updated its risk assessment accordingly.

## Scope

The Guidance applies broadly to all NYDFS-regulated organizations and individuals, using the same jurisdictional reach as Part 500. (As a reminder, the scope of Part 500 changed when regulatory amendments recently went into effect.) Any entity required to hold an NYDFS license falls within its scope, including but not limited to licensed lenders, insurance companies, insurance producers, money transmitters, mortgage servicers, and certain banks.

The Advisory is addressed more narrowly to the chief information security officers (CISOs) of NYDFS-regulated entities. This framing signals that NYDFS views the frontier AI threat as a technical risk that warrants CISO-level ownership, risk assessment, and preventive action.

Though NYDFS may evaluate compliance expectations considering an entity's size, complexity, and risk profile, both documents apply regardless of whether an entity qualifies for a limited exemption under Part 500. The Guidance and Advisory describe best practices rather than regulatory minimums, so the exemption framework that applies to Part 500's mandatory provisions does not carve out any entity from NYDFS's recommendation that it consider these measures, so long as the entity is licensed by NYDFS.

## The Heightened Threat Environment Guidance

The Guidance organizes its recommendations into three categories.

**Reducing the Attack Surface**. Section 1 recommends nine measures, including expedited remediation of known exploited vulnerabilities (with particular emphasis on internet-facing systems), disabling inactive ports and protocols, restricting MFA enrollment changes to authorized processes with strong identity verification, employing phishing-resistant MFA such as hardware tokens or authenticator apps with number matching, network segmentation and geofencing, cloud configuration validation, privileged access reviews, and secure programming practices including input validation and restriction of unsafe script execution.

**Improving Threat Detection and Readiness**. Section 2 covers six measures: confirming that intrusion prevention and endpoint detection tools are current and deployed, verifying that logging and alerting capture anomalous activity, reviewing threat intelligence for indicators of compromise, alerting personnel to active threat campaigns including social engineering, enhancing monitoring of third-party code and applications, and engaging with critical third-party service providers to confirm their awareness and readiness.

**Improving Resilience and Response**. Section 3 addresses five measures: testing backup integrity and recovery time objectives, reviewing and testing incident response and business continuity plans against the specific heightened threat, developing communication strategies for prolonged disruptions, confirming operational technology can function independently, and monitoring financial transactions for sanctions and AML compliance.

## The Frontier AI Advisory

The Advisory builds on the Guidance by identifying frontier AI as a specific trigger for heightened threat posture. NYDFS defines "Frontier AI Models" as AI models that "amplify the potency, scale, and speed of identifying vulnerabilities and exploits in information systems." The Advisory notes these models are not yet broadly available but warns that availability may expand soon.

The Advisory directs regulated entities to Sections 1, 2, and 3.2 of the Guidance and adds four AI-specific recommendations: (1) reassessing vulnerability management timelines because threat actors will exploit AI-discovered vulnerabilities faster, (2) developing dependency maps and coordinating with third-party service providers on downstream risk, (3) applying additional testing and human oversight to AI-generated code before production deployment, and (4) evaluating whether existing logging and alerting capabilities can keep pace with AI-enabled attack cadences.

The Advisory also references NYDFS's October 2024 industry letter on Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks as providing additional relevant considerations.

## Takeaways

The Guidance expressly states that it goes beyond Part 500's minimum controls "in some instances," but does not specify which recommendations exceed current requirements and which merely restate them. Entities conducting gap analyses will need to make that determination provision by provision in light of their own operations. As the Guidance acknowledges, to "determine when and which additional security controls to employ to address specific threat environments, Regulated Entities should assess the specific cybersecurity threat, their Information Systems, supply chain dependencies and usage, as well as sector-specific risks."

Regulated entities could consider the following steps:

- **Update your risk assessment now**. Both publications contemplate that entities will refresh their Part 500 risk assessments to account for frontier AI threats and the current threat environment. This may be a top item that examiners will ask for in supervisory exams.
- **Map the Guidance to your current controls**. Conduct a gap analysis comparing the Guidance's three sections against your existing cybersecurity program. Document where you already comply,

where you exceed the recommendation, and where you have decided not to adopt a measure, with supporting rationale.

- **Brief your CISO on the Advisory**. The Frontier AI Advisory is addressed to CISOs by name. Ensure your CISO has reviewed it and can speak to how the entity's vulnerability management, secure coding, and third-party oversight programs address AI-specific risks.
- **Revisit third-party service provider agreements**. Both the Guidance and the Advisory emphasize downstream dependencies. Cross-reference these publications with NYDFS's October 2025 third-party risk guidance and confirm that your vendor contracts address the scenarios these documents describe.
- **Accelerate vulnerability management timelines**. The Advisory's core message is that AI will compress the window between vulnerability discovery and exploitation. Evaluate whether your current patching and remediation cycles can keep pace.
- **Document everything**. NYDFS will treat these publications as a reference point in examinations. Even where a measure is technically voluntary, the failure to consider it, and to document why you adopted or declined it, creates examination risk.

## Authors

This GT Alert was prepared by:


- Noah N. Gillespie | +1 202.533.2386 | Noah.Gillespie@gtlaw.com
- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Eileen M. Hayes | +1 518.689.1455 | Eileen.Hayes@gtlaw.com