ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / Privacy & Cybersecurity Litigation ADVISORY ■

NOVEMBER 9, 2023

NYDFS Finalizes Second Amendment to Its Cybersecurity Regulation

by *Kristy Brown*, *Kim Peretti*, *Kate Hanniford*, *Ashley Miller*, and *Lance Taubin*

On November 1, 2023, the New York Department of Financial Services (NYDFS) published the finalized Second Amendment to its Cybersecurity Regulation (23 NYCRR Part 500), which includes a number of significant and, for many covered entities, onerous changes to its original regulation. The finalized Second Amendment is much like the June 2023 proposed draft (which made certain revisions to the November 2022 draft). Covered entities should take note of these now-final changes that will require covered entities to review and revamp major components of their cybersecurity programs, policies, procedures, and controls to ensure they are in compliance. This is particularly important as the NYDFS continues to take on an active enforcement role following cyber events, marking itself as a leading cyber regulator in the United States.

Covered entities must notify the NYDFS of certain cybersecurity incidents, including providing notice within: (1) 72 hours after determining a cybersecurity event resulting in the "deployment of ransomware within a material part of the covered entity's information system" occurred; and (2) 24 hours of making an extortion payment in connection with a cybersecurity event.

Covered entities must implement additional cybersecurity controls, including expanding their use of multi-factor authentication and maintaining a comprehensive asset inventory. Covered entities are also required to maintain additional (or more prescriptive) cybersecurity policies and procedures, including ensuring that their incident response plans address specific delineated issues (outlined in the Second Amendment) and maintaining business continuity and disaster recovery plan requirements (both of which must be tested annually).

The most senior levels of the covered entity (senior governing body) must have sufficient knowledge to oversee the cybersecurity program. Additionally, the highest-ranking executive and the CISO are required to sign the covered entity's annual certification of material compliance.

A material failure (which could be a single act) to comply with any portion of the Cybersecurity Regulation for a 24-hour period is considered a violation.

The Second Amendment became effective on November 1, 2023, and covered entities generally have 180 days to come into compliance with the new requirements. There are certain requirements, however, that will be phased in over the next two years. We have outlined the material changes and the effective dates below.

Effective Date	Section	New Requirement in Second Amendment
November 1, 2023	Section 500.19	**Limited exemption.** The NYDFS revised the scope of covered entities eligible for the limited exemption. Small businesses should immediately review the revised limited exemption under Section 500.19. Specifically, the NYDFS increased the minimum number of employees and independent contractors from 10 to 20, the gross annual revenue in each of the last three fiscal years from $5 million to $7.5 million, and the year-end total assets from $10 million to $15 million. Despite the higher thresholds, the number of employees / independent contractors and the gross annual revenue could include non–New York individuals and generated business, expanding the scope to an extent. If the covered entity qualifies for the limited exemption, they are exempt from Sections 500.4; 500.5; 500.6; 500.8; 500.10; 500.14(a)(1), (a)(2), and (b); 500.15; and 500.16. Covered entities will, however, need to implement multi-factor authentication, as noted in Section 500.12, which represents a significant change in the limited exemption under Section 500.19.
	Section 500.20	**Enforcement.** A violation is defined as the "material failure to comply for any 24-hour period with any section" of the Cybersecurity Regulation, which could be a single act or any failure to comply with any portion of the regulation for a 24-hour period. While the NYDFS will consider "the length of time over which [the violation] occurred" in assessing a penalty, suggesting that the NYDFS may be more lenient for a violation over a very short period of time, this revision (and corresponding lack of precision in certain sections) could pose significant risk to covered entities. For example, vulnerability scans and penetration tests frequently identify certain vulnerabilities, and while the Second Amendment states that vulnerabilities must be remediated in a "timely" fashion, it is unclear what those timeframes may be. Covered entities may find it difficult to avoid violating a regulation over a given 24-hour period without further guidance on other aspects of the regulation.

Effective Date	Section	New Requirement in Second Amendment
December 1, 2023	Section 500.17	**Notification of cybersecurity event / cybersecurity incident.** **"Cybersecurity incident."** We note that the NYDFS added "cybersecurity incident" as a defined term in Section 500.1(g). The NYDFS received comments requesting adding this definition to align with the standard nomenclature across the industry. The revisions are, however, more structural than substantive because the NYDFS moved the substantive cybersecurity event reporting requirements from its original regulation (and proposed revisions to Section 500.17(a) from the June 2023 draft) into the definition of "cybersecurity incident." As of December 1, 2023, notice to the NYDFS is triggered by a cybersecurity incident, which encompasses a cybersecurity event (that definition remains unchanged). • "Cybersecurity incident" is defined as "a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that": (1) impacts the covered entity and requires notification to another regulatory/government body; (2) has a "reasonable likelihood of materially harming any material part" of normal operations; or (3) "results in the deployment of ransomware within a material part of the covered entity's information systems." **Ransomware incidents.** Covered entities are now required to notify the NYDFS of cybersecurity events resulting in the deployment of ransomware within a material part of the covered entity's information systems within 72 hours after determining that a cybersecurity incident has occurred. As noted in our prior summaries of the previous proposed drafts, "material" remains undefined. **Extortion payments.** Covered entities must now notify the NYDFS of an extortion payment made in connection with a cybersecurity event within 24 hours of the extortion payment and, within 30 days, provide a written explanation of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable OFAC rules. Note that this reporting requirement applies to any extortion payment, not just extortion payments made in the context of a ransomware event. With this reporting requirement, covered entities will undoubtedly need to take into account any considerations of the attorney-client privilege in conducting an investigation into a cyber-attack.

Effective Date	Section	New Requirement in Second Amendment
April 15, 2024	Section 500.17(b)	**Annual certification of material compliance or acknowledgement of noncompliance.** The NYDFS maintains its current requirement of an annual certification of compliance by a covered entity but has adjusted the standard for certification from "in compliance" to a certification that the covered entity "*materially complied*" with the Cybersecurity Regulation during the prior calendar year. Although the NYDFS does not define material compliance, this revision should provide some flexibility for covered entities to complete the certification. Going forward, covered entities will be presented with two options: (1) submit a written certification that it materially complied with the regulation; or (2) submit a written acknowledgment that it did not "*fully comply*" with the regulation, while also identifying "all sections … that the entity has not materially complied with." It is unclear how the NYDFS intends for covered entities to parse the distinction between material compliance and a lack of full compliance, but the requirement for the covered entity to list each section it was not in material compliance with suggests that it may expect a section-by-section analysis of material compliance as part of the certification process. The NYDFS added an explicit requirement that the CISO *and* the highest-ranking executive (likely the CEO) must sign the certification or acknowledgment – another sign that the NYDFS wants to ensure there is a commitment to complying with the Cybersecurity Regulation from the top.
April 29, 2024	Section 500.2(c)	**Independent audits for Class A covered entities.** The NYDFS specified numerous prescriptive and generally more advanced cybersecurity requirements for large covered entities, called "Class A companies." One requirement includes designing and conducting independent audits of its cybersecurity program based on its risk assessment. Independent audits may be conducted by internal or external auditors, so long as the auditor is free to make their own decisions and not be influenced by the covered entity's owners, managers, or employees. Class A companies have at least $20 million in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the business operations in New York State of the covered entity's affiliates and: (1) have over 2,000 employees; or (2) over $1 billion in gross annual revenue in each of the last two fiscal years. (Section 500.1(d)).

Effective Date	Section	New Requirement in Second Amendment
	Section 500.3*	**Expansion of cybersecurity policies.** The NYDFS expanded the scope of what must be addressed in the covered entity's cybersecurity policies (or written information security plan). Now, the cybersecurity policies and procedures must address (in addition to previously included topics): • Data retention • End-of-life management • Remote access controls • Systems and network monitoring • Security awareness and training • Systems and application security • Incident response and notification • Vulnerability management **Operationalize cybersecurity policies by creating "procedures."** The NYDFS not only requires covered entities to maintain written cybersecurity policies (which must continue to be informed by the covered entity's risk assessment) but now the Second Amendment requires covered entities to also document how such policies are operationalized: "Procedures shall be developed, documented and implemented in accordance with the written policy or policies." Developing, documenting, and implementing procedures in accordance with the covered entity's cybersecurity policy may be a considerable undertaking and require regular oversight and updating as policies evolve. **Review of cybersecurity policies.** The cybersecurity policies must now be reviewed annually (even if there are no changes to the policies) by senior officers or the senior governing body.
	Section 500.5(a)(1), (b), and (c)	**Vulnerability and penetration testing requirements.** The Second Amendment requires covered entities to develop and implement written policies and procedures for vulnerability management. These policies and procedures must, at a minimum, ensure that covered entities conduct penetration testing of information systems from both inside and outside the boundaries by a "qualified internal or external party at least annually."

Effective Date	Section	New Requirement in Second Amendment
	Section 500.9(a)	**Risk assessments.** The NYDFS made only minimal revisions to its risk assessment requirement, adding an explicit requirement for how often covered entities must conduct risk assessments – at a minimum, annually and upon change to business or technology causing a material change to the covered entity's cyber-risk. Under the rationale that the definition of "risk assessment" aligns with industry definitions and standards, the NYDFS declined to incorporate the more prescriptive and tailored definition of "risk assessment" from the November 2022 proposed draft that would have allowed covered entities to "take into account the specific circumstances of the covered entity, including but not limited to its size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors, other relations and their locations, as well as the geographies and locations of its operations and business relations."
	Section 500.11	**Third-Party Service Provider Security Policy.** The NYDFS removed the "limited exception" from developing its own third-party information security policy for an agent, employee, representative, or designee of a covered entity that is itself a covered entity if that agent, employee, representative, or designee follows the covered entity's policy.
	Section 500.14(a)(3)*	**Security awareness training.** Covered entities must conduct annual security awareness training (the frequency of the training was previously not set out in the Cybersecurity Regulation), and the training must now include social engineering training. The addition of an annual requirement and incorporating social engineering content into the training is not a surprise – the NYDFS highlighted the importance of frequent security awareness training, covering social engineering, in prior guidance and enforcement actions.

Effective Date	Section	New Requirement in Second Amendment
November 1, 2024	Section 500.4	**Cybersecurity governance.** The Second Amendment explicitly requires covered entities to designate a CISO (unless exempt under Section 500.19). As a part of the CISO's annual report to the senior governing body (which includes the board of directors or equivalent) on the covered entity's cybersecurity program, the CISO must now include a remediation plan for "material inadequacies." The NYDFS declined to clarify what is meant by "material inadequacies," which all but certainly varies from covered entity to covered entity. The NYDFS's willingness to accept that not all inadequacies (and cybersecurity programs) are equal seems to be at odds with the absence of a more prescriptive and tailored definition of "risk assessment," particularly since the cybersecurity program will be based on the covered entity's risk assessment. The covered entity's CISO must timely report to the covered entity's senior governing body or senior officials any "material cybersecurity issues," such as significant cybersecurity events and significant changes to cybersecurity program. We would note that neither "cybersecurity issues" nor "significant" is defined. The senior governing body must oversee the cybersecurity program and any cyber-risks, requiring the senior governing body to have sufficient understanding of cybersecurity-related matters and confirming that management has allocated sufficient resources to implement and maintain an effective cybersecurity program, among other responsibilities. Notably, in the June 2023 proposed draft, the CISO was empowered with adequate authority to ensure cybersecurity risks are appropriately managed and had the ability to direct sufficient resources to implement and maintain an effective cybersecurity program. The NYDFS pivoted in the final version of the Second Amendment, likely based on persuasive commenters noting that CISOs typically do not have the ability to allocate a company's budget and such responsibility is more appropriate for senior management and the board.

Effective Date	Section	New Requirement in Second Amendment
	Section 500.15	**Encryption.** The current Cybersecurity Regulation requires covered entities to implement controls to protect nonpublic information at rest and in transit, including encrypting nonpublic information (unless infeasible). Under the Second Amendment, covered entities are required to implement encryption that meets industry standards, not the previously utilized broad-based "controls." And while the NYDFS has maintained the infeasibility exception for encryption at rest (allowing effective alternative compensating controls), there is no such carve-out for encryption of nonpublic information in transit.
	Section 500.16	**Incident response plan and business continuity and disaster recovery plan.** Covered entities' incident response plans now must address "preparation of root cause analysis that describe[] how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence." It is unclear, however, what format and level of detail the NYDFS would require in a root cause / business impact analysis. As with Section 500.17, this requirement will require a close consideration of the attorney-client privilege when covered entities direct an investigation into a cyber-attack. The NYDFS also implemented detailed business continuity and disaster recovery plan (BCDR) specifications, requiring BCDR plans to include minimum information, like identifying documents, systems, and personnel that are critical to continue operations, as well as procedures for maintaining offsite backups and the timely recovery of critical data (which the NYDFS does not define) and information systems and resuming operations as soon as reasonably possible following a cybersecurity-related disruption to normal business activities. Covered entities are likewise required to: (1) ensure the plans are distributed or otherwise accessible to all employees necessary to implement the plans; (2) train all employees responsible for implementing the plans; (3) at least annually test the incident response and BCDR plans with staff and management critical to the response and the ability to restore its critical data and information systems; and (4) maintain backups necessary to restore material operations.

Effective Date	Section	New Requirement in Second Amendment
May 1, 2025	500.5(a)(2)	**Vulnerability scanning.** Covered entities are now required to conduct automated vulnerability scans and manual review of any systems not otherwise covered by automated scans. The cadence for reporting and remediating vulnerabilities identified by automated/manual vulnerability scans should be established in the covered entity's risk assessment.

	Section 500.7*	**Access controls.**
		
		The Second Amendment added prescriptive access control protocols, including the requirements to:
		• Limit access to information systems that provide access to nonpublic information to only "need to know" individuals.
		• Implement enhanced privileged account access requirements, including limiting the number of privileged accounts, and use of privileged accounts to only when performing privileged functions.
		• Review (at least annually) access controls/privileges and remove or disable stale accounts.
		• Disable or securely configure all remote control protocols.
		• Promptly terminate access of terminated personnel.
		• Implement a reasonable written password policy.
		• Class A companies must also:
		  • Implement a privileged access management solution.
		  • Monitor privileged access activity.
		  • Implement an automated method for blocking commonly used passwords.

	Section 500.14(a)(2) and (b)	**Monitoring and logging.** Covered entities must now specifically implement risk-based controls designed to protect against malicious code, including monitoring and filtering web traffic and blocking malicious email content. Class A companies must also implement the following (or a reasonably equivalent / more secure compensating control approved by the CISO in writing): • Endpoint detection and response tool. • Centralized logging and security event alerting tool.

Effective Date	Section	New Requirement in Second Amendment
November 1, 2025	Section 500.12*	**Expanded MFA requirements.** As noted in its earlier proposed amendments, the NYDFS has moved away from its "external access to internal network" definition to more closely align with the FTC's Safeguards Rule, requiring multi-factor authentication (MFA) for "any individual accessing any information systems of a covered entity." The NYDFS removed from Section 500.12(a) both (1) the prerequisite that MFA be implemented based on the covered entity's risk assessment; and (2) the option of implementing other effective controls, such as risk-based authentication. By doing so, the NYDFS emphasizes the importance of expanding MFA, despite retaining the limited exception if the CISO approves in writing a reasonably equivalent or more secure compensating controls (that must be reviewed periodically, and at least annually). Interestingly, the NYDFS noted that while MFA would not be required for individuals accessing a covered entity's public website because the public website is not considered part of the covered entity's information system, if a customer logs into a covered entity's online portal from a public-facing website, that portal would be considered the covered entity's information system and thus MFA would be required. (See "Assessment of Public Comments on the Revised Proposed Second Amendment to 23 NYCRR Part 500," p. 21-22). **MFA for small businesses.** Covered entities that qualify for a limited exemption under Section 500.19(a) are no longer exempt from deploying MFA because they must implement MFA on: • Remote access to the covered entity's information systems (similar to the previous Section 500.12(b)). • Remote access to third-party applications (including cloud-based applications) where nonpublic information is accessible. • All privileged accounts (except service accounts that prohibit interactive logins). The NYDFS has put a heavy emphasis (both in the Second Amendment and in its guidance/enforcement mechanisms) on MFA as an effective and inexpensive method of reducing cyber-risks. It is no surprise that small businesses will now be required to implement MFA to a certain extent.

Effective Date	Section	New Requirement in Second Amendment
	Section 500.13(a)	**Asset inventory.** One of the most significant changes to the Cybersecurity Regulation in the Second Amendment is the requirement to maintain policies and procedures to "maintain a complete, accurate and documented asset inventory" that includes a method to track key information for each assist, including the "(i) owner; (ii) location; (iii) classification or sensitivity; (iv) support expiration date; and (v) recovery time objectives." This new requirement is not limited to certain assets, such as corporate-owned devices or certain assets accessing nonpublic information. The NYDFS seems to build off the existing requirement to maintain an asset inventory policy (Section 500.3(c)) to offer more prescriptive asset management requirements, emphasizing the importance of maintaining visibility of the covered entity's assets in one location (which can itself be a challenge given the variety of systems and assets maintained by many covered entities) and potential vulnerability.
*Not applicable to covered entities that qualify for exemptions, including entities that do not maintain nonpublic information (Section 500.19(c)) and captive insurers (Section 500.19(d)).		

The NYDFS is providing a number of resources for covered entities, including a helpful visual overview of the implementation timeline for covered entities, Class A companies, and small businesses (NYDFS-licensed individual producers, mortgage loan originators, and other businesses that qualify for exemptions under Sections 500.19 (a), (c), and (d)). The NYDFS is also hosting a series of webinars to provide an overview of the Second Amendment; individuals can register for the webinars on the NYDFS's website.

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team** or **Privacy & Cybersecurity Litigation Team**.

Privacy, Cyber & Data Strategy:

Kim Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Kate Hanniford
+1 202 239 3725
kate.hanniford@alston.com

Lance Taubin
+1 212 905 9301
lance.taubin@alston.com

Litigation/Enforcement:

Kristy Brown
+1 404 881 7584
kristy.brown@alston.com

Ashley Miller
+1 404 881 7831
ashley.miller@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: Vantage South End ■ 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: City Center Fort Worth ■ Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7DE ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333