GIBSON DUNN

# New York Department of Financial Services Finalizes Second Amendment to Cybersecurity Regulation

Client Alert | December 18, 2023

---

*The Second Amended Cybersecurity Regulation signals a significant shift in the cybersecurity regulatory landscape, reflecting NYDFS's proactive efforts to empower covered entities to protect themselves against escalating threats of sophisticated and frequent cyber events.* On November 1, 2023, the New York Department of Financial Services ("NYDFS" or "the Department") finalized the amendments to its Part 500 Cybersecurity Regulation (the "Second Amended Cybersecurity Regulation") and cemented its status as a proactive regulatory leader in the effort to protect consumer data, promote cybersecurity governance best practices, and keep pace with new cybersecurity threats and emerging technology. In line with NYDFS's risk-based approach to cybersecurity, and as previewed in its previous drafts, the Second Amended Cybersecurity Regulation introduces several notable changes, including expanded responsibility for senior governing bodies, obligations to implement additional safeguards, new requirements for larger companies, new and increased obligations related to written policies and procedures, heightened requirements around audits and risk assessments, and additional reporting requirements for cybersecurity incidents. NYDFS's cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation"), was first released in March 2017 and went into full effect in March 2019. A minor, ministerial amendment changing the date of the required annual certification was made in 2020 (the "First Amended Cybersecurity Regulation"). In July of 2022, NYDFS began the process of a thorough review and update to the regulation. Since then, NYDFS has issued three draft amendments—the initial Draft Proposed Second Amendment (published July 29, 2022), the Proposed Second Amendment (published November 9, 2022), and the Revised Proposed Second Amendment (published June 28, 2023)—and held two notice and comment periods with active stakeholder participation. Key updates to the Cybersecurity Regulation, as reflected in the Second Amended Cybersecurity Regulation, are highlighted below:

1. **Heightened Obligations for Senior Leadership and Governing Bodies**

Under the Second Amended Cybersecurity Regulation, the "senior governing body" of a covered entity joins the Chief Information Security Officer ("CISO") at the helm of the company's cybersecurity apparatus. "Senior governing body" is broadly defined to account for the varied sizes, corporate structures, business models, and industries under NYDFS's purview. A covered entity's board of directors or equivalent governing body, a board committee, or senior officer(s) responsible for the entity's cybersecurity program would all qualify as senior governing bodies under the updated regulation. The senior governing body of a covered entity is required to exercise oversight of the covered entity's cybersecurity risk management. At a minimum, this entails (i) having a sufficient understanding of cybersecurity-related matters; (ii) requiring management to develop, implement, and maintain the covered entity's cybersecurity program; (iii) regularly receiving and reviewing management reports on cybersecurity; and (iv) confirming that sufficient resources are allocated in order to implement and maintain the cybersecurity program. Previously, a covered entity's CISO was charged with ensuring sufficient allocation of resources to develop and maintain an effective cybersecurity system; in recognition of the fact that senior governing bodies, not CISOs, tend to make enterprise-

## Related People

Stephenie Gosnell Handler

Vivek Mohan

Sara K. Weed

Anne Lonowski

Ruby B. Lang

wide resource allocation decisions, NYDFS shifted that responsibility to the senior governing body. The Second Amended Cybersecurity Regulation also expands reporting obligations on the CISO, requiring the timely reporting of material cybersecurity issues to the senior governing body or senior officer(s), such as significant cybersecurity events and significant changes to the cybersecurity program.

2. **Increased Investment in Cybersecurity Programs**

The Second Amended Cybersecurity Regulation requires covered entities assess the adequacy of their governance practices and their investments in technology and personnel. In addition to significantly expanding the breadth of covered entities' cybersecurity efforts by including "nonpublic information stored on the covered entity's information systems" in its definition of "cybersecurity program," NYDFS established additional requirements related to written policies and procedures. Companies must have written incident response plans, business continuity and disaster recovery plans, and plans for investigating and mitigating cybersecurity events. As it did in the original Cybersecurity Regulation in 2017 for the then-novel incident response plans, NYDFS took care to enumerate a number of proactive measures intended to help covered entities formulate effective business continuity plans. The draft amendments related to business continuity and incident response plans remained largely the same throughout the process of reviewing and updating the regulation, though the Department did make a few practical and logistical changes. Each covered entity must also implement written policies and procedures that are designed to produce and maintain a complete, accurate, and documented asset inventory of its information systems. NYDFS made a subtle adjustment to this provision from the June 2023 Revised Proposed Second Amendment, requiring covered entities to "produce and maintain" an asset inventory rather than "ensure" it exists—this is one of many instances where the Department made revisions geared toward providing covered entities with concrete guidance on how to navigate the cybersecurity landscape.

3. **Separate Requirements for Larger "Class A" Companies**

NYDFS codified heightened cybersecurity requirements for a newly defined class of larger entities, termed "Class A" companies. Throughout its drafting process, NYDFS iterated upon the scope and scale of Class A companies, and ultimately chose a relatively limited definition. Class A companies are those with an in-state gross annual revenue over $20 million in each of the last two fiscal years, and have had either (i) an average of more than 2,000 employees, or (ii) over $1 billion in gross annual revenue in each of the last two fiscal years. When calculating these figures, entities should include any affiliates that it shares information systems, cybersecurity resources, or a cybersecurity program with. The Department has imposed several obligations on Class A companies, including to design and conduct independent audits of their cybersecurity programs based upon their respective risk assessments; monitor privileged access activity and implement privileged use management solutions; and implement security precautions such as centralized logging and notifications for security alerts, automatic rejection of common or simple passwords, and endpoint detection and response solutions for anomalous activity. While the Revised Proposed Second Amendment published on June 28, 2023 would have required audits of Class A cybersecurity programs on an annual basis, the final Second Amended Cybersecurity Regulation introduces some flexibility by requiring audits at a frequency determined by the results of the entity's risk assessments. This change reflects the Department's understanding that designing and conducting annual audits may be a particularly burdensome, time-consuming, and resource-heavy endeavor given the size of Class A companies and the complexity of their cybersecurity programs. NYDFS did, however, add that Class A companies should *design* their audits, in addition to conducting them, which demonstrates NYDFS's desire for covered entities to be engaged, comprehensive, and diligent about their cybersecurity efforts.

4. **Additional Requirements for Audits and Risk Assessments**

In earlier draft amendments, NYDFS had proposed strict requirements related to audits, risk assessments, and penetration tests, such as prohibiting the use of internal auditors and requiring covered entities retain external auditors. Many public commenters took issue with these proposals; in response, the Department expanded the pool of eligible auditors and experts to include internal personnel and reduced the rigidity of timetables for certain obligations. Under the Second Amended Cybersecurity Regulation:

- An "independent" audit is one conducted by internal or external auditors, who are free to make their own decisions and are not influenced by the covered entity or its owners, managers, or employees;
- Class A companies must re-review and update their risk assessments at least annually, and whenever changes to their business or technology result in a "material change" to the cyber risk they face;[1] and
- Penetration testing of information systems must be performed annually by qualified internal or external "parties" (not necessarily by "experts," as contemplated in the Proposed Second Amendment).

In addition, the Second Amended Cybersecurity Regulation includes a new requirement that risk assessments must "inform the design" of the cybersecurity program and enable adjustments in controls to address evolving cybersecurity and privacy risks. This includes general risks and those particular to the covered entity's business operations.

5. **Incident Notification Obligations**

Covered entities should take note of the growing number and increased sophistication of cybersecurity events in recent years. In an effort to combat these threats, NYDFS established a new 24-hour notification obligation in the event a covered entity makes a ransom payment, and a 30-day window for covered entities to provide a written description of why the payment was necessary, alternatives to payment that were considered, and all diligence conducted to ensure compliance with applicable rules and regulations. NYDFS narrowed the circumstances for which covered entities would have to provide NYDFS with notice by differentiating between "cybersecurity events" and "cybersecurity incidents." Under the Second Amended Cybersecurity Regulation, entities must notify NYDFS only where the covered entity has determined that there is an incident at the covered entity, its affiliate, or a third-party service provider that: (i) impacts the covered entity and has triggered the notification requirement of another governmental body, self-regulatory agency, or other supervisory body; (ii) has a reasonable likelihood of materially harming normal operations of the covered entity; or (iii) results in the deployment of ransomware within a material part of the covered entity's information systems. NYDFS considered, but did not adopt, a requirement that entities notify the Department of any incident involving unauthorized access to a "privileged account,"[2] acknowledging that such an overbroad requirement would likely lead to overreporting and the inefficient use of resources.

6. **Compliance Timeline**

In general, entities have 180 days, or until April 29, 2024, to comply with the Second Amended Cybersecurity Regulation. However, several provisions have different specified transitional periods that override this general timeline:

- Incident reporting requirements take effect 30 days after the effective date of the Second Amended Cybersecurity Regulation, or December 1, 2023.
- Governance, encryption, incident response plan and business continuity management, and the limited exemption provisions take effect one year after the effective date of the Second Amended Cybersecurity Regulation, or November 1, 2024.
- Vulnerability scanning, access privileges and management, and monitoring and training provisions take effect 18 months after the effective date of the Second Amended Cybersecurity Regulation, or May 1, 2025.
- Multifactor authentication and asset management and data retention provisions

take effect two years after the effective date of the Second Amended Cybersecurity Regulation, or November 1, 2025.

**Looking Ahead** The proliferation of artificial intelligence ("AI"), generative AI, and large language models is on NYDFS's radar[3] and may receive attention in a forthcoming round of amendments. Although NYDFS declined to dedicate a section of the Cybersecurity Regulation to these rapidly expanding technologies, it cautioned covered entities that cybersecurity risks associated with AI are "concerning" and should be taken into account in risk assessments and addressed in cybersecurity programs.[4] The Second Amended Cybersecurity Regulation signals a significant shift in the cybersecurity regulatory landscape, reflecting NYDFS's proactive efforts to empower covered entities to protect themselves against escalating threats of sophisticated and frequent cyber events. Organizations should assess their cybersecurity policies and practices to ensure that adequate controls, resources, and personnel are in place to comply with NYDFS's regulatory changes. _____ [1] NYDFS did not adopt its proposed requirement that external experts conduct risk assessments at least once every three years. [2] Privileged account means "any authorized user account or service account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change or remove other accounts, or make configuration changes to information systems." Section 500.1(n). [3] Assessment of Public Comments on the Revised Proposed Second Amendment to 23 NYCRR Part 500, here. [4] Assessment of Public Comments on the Revised Proposed Second Amendment to 23 NYCRR Part 500, here.

---

The following Gibson Dunn lawyers assisted in preparing this alert: Alexander Southwell, Stephenie Gosnell Handler, Vivek Mohan, Sara Weed, Cassarah Chu, Anne Lonowski, and Ruby Lang.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity & Data Innovation practice group: **United States** S. Ashlie Beringer – Co-Chair, Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Alexander H. Southwell – Co-Chair, New York (+1 212.351.3981, asouthwell@gibsondunn.com) Matthew Benjamin – New York (+1 212.351.4079, mbenjamin@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202.887.3786, dburns@gibsondunn.com) Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com) Lauren R. Goldman – New York (+1 212.351.2375, lgoldman@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com) Howard S. Hogan – Washington, D.C. (+1 202.887.3640, hhogan@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415.393.8395, klinsley@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Karl G. Nelson – Dallas (+1 214.698.3203, knelson@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com) Ashley Rogers – Dallas (+1 214.698.3316, arogers@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com) Benjamin B. Wagner – Palo Alto (+1 650.849.5395, bwagner@gibsondunn.com) Sara K. Weed – Washington, D.C. (+1 202.955.8507, sweed@gibsondunn.com) Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415.393.8333, mwong@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com) **Europe** Ahmed Baladi – Co-Chair, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com) **Asia** Connell O'Neill – Hong Kong (+852 2214 3812,

coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com) 

## Related Capabilities

Privacy, Cybersecurity, and Data Innovation

Artificial Intelligence