GIBSON DUNN

New York State Department of Financial Services Meaningfully Rachets Up Cyber Requirements with New Draft Amendments

Client Alert | August 8, 2022

On July 29, 2022, the New York Department of Financial Services ("DFS") released Draft Amendments to its Part 500 Cybersecurity Rules; the Draft Amendments would update the Cybersecurity Rules in a manner consistent with the "catalytic" role it took in 2017 as the first state to codify certain cybersecurity best practices and guidance into explicit regulatory requirements for covered entities. The cybersecurity landscape has evolved in the past five years, and the Draft Amendments demonstrate that DFS continues to take a forward-leaning role in strengthening cybersecurity practices. The Draft Amendments propose increased expectations for senior leaders, heightened technology requirements, an expanded set of events covered under the mandatory 72-hour notification requirements, a new 24-hour reporting requirement for ransom payments and a 30-day submission of defenses, significant new requirements for business continuity and disaster recovery, and heightened annual certification and assessment requirements. Notably, the amended regulations propose a new class comprising larger entities which will be subject to increased obligations for their cybersecurity programs. Even the definition of a cybersecurity program has been expanded to include coverage of nonpublic information stored on those information systems—a substantial increase in covered information that will have significant downstream effects on reporting and certification requirements. The cybersecurity regulations by DFS were first released in March 2017 and went into full effect in March 2019, as previewed in our prior alert and subsequently discussed in our agency round-ups (2020 & 2021).

Key provisions of the Draft Amendments are highlighted below.

1. **More Stringent Notification Obligations**

The Draft Amendments establish additional requirements on top of DFS's existing 72-hour notification requirements, including:

- Requiring notification to DFS within 72 hours of unauthorized access to privileged accounts or the deployment of ransomware within a material part of the company's information systems. These are in addition to the existing requirements to notify DFS within 72 hours of any cybersecurity events that require notice to a supervisory body or that have a reasonable likelihood of materially harming a material part of the company's normal operations. Notably, these newly proposed requirements would significantly lower the notification threshold, as they could be triggered before any sign of actual data compromise or exfiltration.
- A new 24-hour notification obligation in the event a ransom payment is made, and a 30-day requirement to provide a written description of why the payment was necessary, alternatives to payment that were considered, and all sanctions

Related People

Stephenie Gosnell Handler

Terry Wong

diligence conducted.

2. **Heightened Requirements for Larger "Class A" Companies**

Adhering to the mantra "with great data comes great responsibility," the Draft Amendments also increase cybersecurity obligations for a newly defined class of larger entities, which are under DFS's authority. These "Class A" companies are defined as entities with over 2,000 employees or over $1 billion in gross annual revenue average over the last three years from all business operations of the company and its affiliates. Under the Draft Amendments, Class A companies are required to comply with heightened technical requirements as well as risk assessments and audits. They must:

- Conduct weekly systematic scans or reviews reasonably designed to identify publicly known cybersecurity vulnerabilities, and document and report any material gaps in testing to the board and senior management;
- Implement an endpoint detection and response solution to monitor anomalous activity and a solution that centralizes logging and security event alerting;
- Monitor access activity and implement a password vaulting solution for privileged accounts and an automated method of blocking commonly used passwords;
- Conduct an annual, independent audit of their cybersecurity programs; and
- Use external experts to conduct a risk assessment at least once every three years.

3. **Increased Obligations on Company Governing Bodies**

The original Part 500 regulations imposed a number of new obligations on companies' governing bodies, including the need for a chief information security officer ("CISO") or equivalent personnel, detailed cybersecurity reporting to the board, and written policies approved by a senior officer. The Draft Amendments enhance in a very meaningful way many of the Part 500 governance requirements, further indicating how important DFS views strong governance in the quest for effective cybersecurity. The Draft Amendments include obligations:

- To ensure the boards of covered entities have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cyber risk;
- To provide the CISO with adequate independence and authority to appropriately manage cyber risks;
- That the CISO will provide the board with additional detailed annual reporting on plans for remediating issues and material cybersecurity issues or events;
- That the CISO will annually review the feasibility of encryption and the effectiveness of any compensating controls for any unencrypted nonpublic information;
- That covered entities' cybersecurity policies must be approved by the board on an annual basis; and
- That add significantly to the annual certification requirements, requiring covered entities to not only certify to their compliance or acknowledge any noncompliance, but also provide sufficient data and documentation to accurately determine and demonstrate compliance, and have such certification or acknowledgment of noncompliance be signed by both the CEO and the CISO.

The Draft Amendments also provide an option for covered entities to submit written acknowledgement that, for the prior calendar year, they did not fully comply with their cybersecurity obligations. Covered entities who submit this acknowledgment will be required to identify all the provisions of the compliance rules that were not followed,

describe the nature and extent of the noncompliance, and identify all the areas, systems, and processes that require material improvement, updating, or redesign.

These additional reporting requirements are substantial, and would greatly increase the burden on CEOs, CISOs, and other personnel involved in the preparation of these annual certifications or acknowledgements.

4. **Expanded Requirements for Operational Resilience and Incident Response**

The Draft Amendments expand measures directed at "operational resilience" beyond incident response plans, requiring covered entities to also have written plans for business continuity and disaster recovery ("BCDR"). Notably, the original Part 500 cybersecurity regulations were the first of its kind to stipulate detailed requirements for cybersecurity incident response plans. Again, DFS is breaking similar ground with BCDR plans, requiring proactive measures to mitigate disruptive events by, at a minimum:

- Identifying business components essential to continued operations (documents, data, facilities, personnel, and competencies) and personnel responsible for implementation of the BCDR plans;
- Preparing communications plans to ensure continuity of communications with various stakeholders (leadership, employees, third parties, regulatory authorities, others essential to continuity);
- Maintaining procedures for the back-up of infrastructure and data; and
- Identifying third parties necessary to continued operations.

Furthermore, DFS has proposed a significant revision to its requirements for incident response plans, requiring that they differentiate based on incident type (e.g., ransomware), while continuing to require that such plans address the previously enumerated areas (e.g., internal response processes; incident response plan goals; definitions of clear roles, responsibilities and levels of decision-making authority; communications and information sharing; identification of remediation requirements; documentation and reporting, etc.) as well as the newly added requirement to address recovery from backups.

Under the Draft Amendments, relevant personnel must receive copies of the incident response plan and BCDR plan, copies must be maintained offsite, and all personnel involved in implementation of the plans must receive appropriate training. In addition, covered entities are required to conduct incident response and BCDR exercises.

5. **Enhanced Technology and Policy Requirements**

The Draft Amendments strengthen technical requirements and written policy requirements for covered entities, codifying certain best practices in key cyber risk areas. The Draft Amendments specifically:

- Clarify the definition of "privileged accounts" as covering any account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, or affect a material change to technical or business operations. Under the proposals, privileged accounts must:
    - Have multi-factor authentication (with exceptions for certain service accounts); and
    - Be limited in both number and access functions to only those necessary to perform the user's job;
    - Be limited in use to only when performing functions requiring their use of such access;
- Require stricter access management, including periodic review of all user access

privileges and removal of accounts and access that are no longer necessary, as well as disabling or securely configuring all protocols that permit remote control of devices;

- Require that emails are monitored and filtered to block malicious content from reaching authorized users;
- Mandate penetration testing be conducted by an independent party at least annually, and also adjust the required frequency of vulnerability assessments from bi-annually to "regular[ly]," with Class A companies conducting weekly scans as noted above;
- Require the use of strong, unique passwords—and Class A companies have additional requirements, as discussed above, relating to passwords and monitoring of access activity;
- Require multi-factor authentication for remote access to the network and enterprise and third-party applications that access nonpublic information; and
- Mandate that covered entities must maintain backups isolated from network connections.

The Draft Amendments also contain new measures for asset inventory and management, which may cost companies significant time and resources to implement. These measures require all covered entities to:

- Implement written policies and procedures to ensure a complete and documented asset inventory for all information systems and their components (e.g., hardware, operating systems, applications, infrastructure devices, APIs, and cloud services); and
- Have asset inventory that must, at a minimum, track each asset's key information (e.g., owner, location, classification or sensitivity, support expiration date, and recovery time requirements).

The Draft Amendments further require additional written cybersecurity policies to include procedures for end of life management, remote access, and vulnerability and patch management. Notably, despite the prominence of recent supply chain cybersecurity attacks, there are not substantive changes to the Part 500 requirements relating to third-party service providers.

6. **Increased Requirements for Risk Assessments, Impact Assessments**

The Draft Amendments further expand the requirements for and definition of "risk assessment" to make clear that they must be:

- Tailored to consider the "specific circumstances" of the covered entity, including 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; and
- Updated at least annually.

While DFS has not changed the core cybersecurity functions that must be covered by the risk assessment per se, covered entities will need to ensure that it covers the broadened scope of "cybersecurity program" under the Draft Amendments (nonpublic information stored on the covered entity's information systems). Furthermore, another substantial proposal is the requirement that covered entities must conduct impact assessments whenever a change in the business or technology causes a material change to the covered entity's cyber risk.

7. **Clarified Enforcement Considerations**

Finally, the Draft Amendments contain two significant clarifications regarding the enforcement of the Part 500 Cybersecurity Rules:

- A violation occurs by committing any act prohibited by the regulations or failing to satisfy a required obligation. This includes the failure to comply for more than 24 hours with any part of the regulations or the failure to prevent unauthorized access to nonpublic information due to noncompliance with the regulations.
- DFS may consider certain aggravating and mitigating factors when assessing the severity of penalties, including: cooperation, good faith, intentionality, prior violations, number or pattern of violations, gravity of violation, provision of false or misleading information, harm to customers, accuracy and timeliness of customer disclosures, participation of senior management, penalties by other regulators, and business size.

Next Steps

This report is not an exhaustive list of the changes contained in the Draft Amendments, but it provides a high-level overview of the impact of the Draft Amendments on the Part 500 Cybersecurity Rules, should they be adopted. These recent Draft Amendments will go through a short pre-proposal comments period, which ends on August 18, 2022. After official publication of the proposed amendments, there will be a 60-day comment period. Pending further revisions, most of the amendments would take effect 180 days after adoption, while some requirements—i.e., notification requirements and changes to annual notice of certification—would take effect on an expedited timeframe of 30 days after adoption. Other requirements (e.g., regarding access controls) would take effect a year after adoption.

These amendments signal DFS's continued focus on ensuring the Part 500 Cybersecurity Rules continue to raise the regulatory bar on covered entities' cybersecurity programs in an era of a rapidly evolving cyber threat landscape. While many of the Draft Amendments reflect the current state of best practice guidance, covered entities will need to intentionally review the Draft Amendments and ensure they are well-positioned from a governance, technology, and budgetary perspective to ensure compliance.

This alert was prepared by Alexander H. Southwell, Stephenie Gosnell Handler, Terry Wong, and Dustin Stonecipher*.

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 Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com) S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@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) 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) Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com) H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com) Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com) Alexander H. Southwell – Co-Chair, PCDI Practice, New York

(+1 212-351-3981, asouthwell@gibsondunn.com) Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@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) Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Europe Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com) Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Bernard Grinspan – Paris (+33 (0) 1 56 43 13 00, bgrinspan@gibsondunn.com) Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com) Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)

Asia Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com) Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

** Dustin Stonecipher is an associate working in the firm's Washington, D.C. office who is admitted only in Maryland.*

Related Capabilities

Privacy, Cybersecurity, and Data Innovation