SULLIVAN & CROMWELL LLP

S&C memo

August 15, 2022

New York State Department of Financial Services Releases Pre-Proposed Amendments to Cybersecurity Regulations

Agency Considers Expanding Protections Covered Entities Are Required to Implement, Including Additional Cybersecurity Measures for Large Covered Entities

SUMMARY

On July 29, 2022, the New York State Department of Financial Services ("DFS") released so-called pre-proposed amendments ("Amendments") to DFS's Cybersecurity Requirements for Financial Services Companies ("Cybersecurity Regulation").[1] The period for "outreach" comments to the amendments ends Thursday, August 18, 2022, after which DFS may officially publish its amendments to the Cybersecurity Regulation in the State Register, triggering a 60-day formal notice-and-comment period. The Amendments represent a comprehensive update of the existing cybersecurity requirements to which Covered Entities are subject.[2] Among other things, the Amendments would (1) require Covered Entities to notify the DFS Superintendent within 24 hours of making an "extortion payment" as a result of a cybersecurity event, and within 30 days provide the Superintendent with written information concerning the decision to make such payment, (2) require Covered Entities to implement a business continuity and data recovery plan in addition to incident response plans, and (3) establish additional auditing, reviewing, and monitoring requirements for a new classification of "Class A" companies—Covered Entities that, together with their affiliates, have over 2,000 employees or over $1 billion in average annual gross revenue over the preceding three fiscal years.

Under the draft Amendments, Covered Entities would need to bring, subject to certain exceptions, their cybersecurity programs into compliance with the amended Cybersecurity Regulation within 180 days of publication of the Notice of Adoption in the State Register.

BACKGROUND

The currently effective iteration of the Cybersecurity Regulation, setting "certain regulatory minimum standards . . . designed to promote the protection of customer information as well as the information technology systems of regulated entities," became effective on March 1, 2017.[3] The Cybersecurity Regulation has "served as a model for other regulators, including the U.S. Federal Trade Commission, multiple states, and the National Association for Insurance Commissioners ('NAIC')."[4] DFS last issued new guidance on Covered Entities' minimizing ransomware risks and vulnerabilities on June 30, 2021 (the "June 2021 Guidance").

The DFS's release of the Amendments comes in the wake of significant federal legislative and regulatory activity in the realm of cybersecurity. For example, on November 18, 2021, the Board of Governors of the Federal Reserve System ("Federal Reserve System"), Office of the Comptroller of the Currency ("OCC"), and Federal Deposit Insurance Corporation ("FDIC") issued a final rule mandating regulatory reporting of certain cybersecurity events ("Federal Rule"). The Federal Rule, which became effective on April 1, 2022,[5] requires a banking organization to notify its primary banking regulator within 36 hours of a "computer-security incident" which has or is reasonably likely to disrupt or degrade the banking organization's: (i) ability to carry out banking activities for a material portion of its customer base; (ii) business lines the failure of which would result in a material loss of revenue, profits, or franchise value; or (iii) operations the failure of which would pose a threat to the financial stability of the United States.[6] Moreover, on March 15, 2022, President Biden signed into law the Strengthening American Cybersecurity Act of 2022, which requires entities in the critical infrastructure sector to report both covered cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency ("CISA"). Finally, on March 9, 2022, the Securities and Exchange Commission proposed new cybersecurity disclosure rules for public companies (the "Proposed SEC Rules"), which address topics including disclosure of material cybersecurity incidents, as well as cybersecurity risk management, strategy and governance.

While the Amendments align with some of the recommendations set forth in the June 2021 Guidance, in other ways they go beyond it. While the June 2021 Guidance focused on companies' ransomware attack preparedness, the Amendments represent updates to DFS's requirements for Covered Entities related to cybersecurity event notification, written cybersecurity policies, and cybersecurity testing and auditing, among other changes. The Amendments also designate a category of "Class A" companies subject to heightened cybersecurity requirements. Furthermore, the 24-hour notification window is not present in the Insurance Data Security Model Law adopted by the NAIC,[7] contributing to a growing patchwork of regulatory notification requirements applicable to banking and insurance organizations.

OVERVIEW OF THE POTENTIAL AMENDMENTS

The Amendments would place new requirements for Covered Entities to provide notification to the Superintendent of information about certain cybersecurity incidents and to enhance cybersecurity protections in several ways, including the manner in which Covered Entities implement cybersecurity policies and procedures, the testing Covered Entities employ to ensure the efficacy of their cybersecurity regimes, and the training provided to employees or Covered Entities.

A. REQUIRED NOTIFICATION TO DFS REGARDING CERTAIN CYBERSECURITY INCIDENTS

The Amendments contemplate new requirements to provide notification to DFS regarding certain cybersecurity incidents. Under the amended Section 500.17, a Covered Entity's notice requirements would be expanded to include:

1. Notifying the DFS Superintendent within 72 hours of cybersecurity events (i) where an unauthorized user gains access to any privileged account or (ii) that resulted in the "deployment of ransomware within a material part of the [C]overed [E]ntity's information system."[8]
2. Notifying the Superintendent within 24 hours of making an "extortion payment" in connection with a cybersecurity event.[9]
3. Within 30 days of an extortion payment, providing the Superintendent a "written description 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 rules and regulations including those of the Office of Foreign Assets Control."[10]

The requirement to provide notice of unauthorized user access to a privileged account, or any deployment of ransomware within a material part of the information system, simply formalizes the portion of the June 2021 Guidance stating that DFS intends for Covered Entities to provide notice of such matters under Section 500.17.

B. REQUIRED CERTIFICATIONS TO DFS

The Amendments would also add documentation requirements to the process by which Covered Entities are required to confirm their compliance with the Cybersecurity Regulation on an annual basis.[11] Each Covered Entity is currently required to submit a written certification of compliance to the Superintendent by April 15 each year concerning the prior calendar year. The Amendments clarify that this written notice should be based on "data and documentation sufficient to accurately determine and demonstrate such full compliance, including, to the extent necessary, documentation of officers, employees, representatives, outside vendors, and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules, or otherwise."[12] Alternatively, a Covered Entity could submit a written acknowledgement by April 15 identifying (i) the specific Cybersecurity Regulation provisions with which the

Covered Entity was not in full compliance in the previous year, and (ii) the areas, systems, and processes requiring material improvements.[13]

C. "OPERATIONAL RESILIENCE" PLANS

The Amendments to Section 500.16, which currently describes the incident response plans that Covered Entities are required to implement, would now focus on broader "[o]perational [r]esilience," encompassing enhanced incident response plan requirements and a new required business continuity and disaster recovery ("BCDR") plan. The amended Section 500.16 would also require Covered Entities to maintain backups isolated from network connections, periodically test their ability to restore systems from backups, and address in the incident response plan the topics of backup recovery and updating the incident response plan as necessary.[14]

BCDR Plan. The required BCDR plan would need to be reasonably designed to ensure the availability and functionality of a Covered Entity's services and protect the Covered Entity's personnel, assets, and nonpublic information in the event of an emergency or disruption. To this end, the BCDR plan would need to, at minimum:

1. Identify documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operations of the Covered Entity's business;
2. Identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;
3. Include a plan to communicate with essential persons in the event of an emergency or other disruption to the operations of the Covered Entity;
4. Include procedures for the maintenance of backup facilities, systems, and infrastructure as well as alternative staffing and other resources to enable the timely recovery of data and documentation and to resume operations as soon as reasonably possible following a disruption to normal business activities;
5. Include procedures for the backup or copying, with sufficient frequency, of documents and data essential to the Covered Entity's operations and offsite information storage; and
6. identify third parties necessary to the continued operations of the Covered Entity's business.[15]

A Covered Entity would be required to distribute copies of both the incident response plan and BCDR plan to all relevant employees, provide relevant training on the plans to all employees, and periodically test both the incident response plan and BCDR plan.[16] This dissemination requirement departs from federal regulations and guidance concerning, for example, disaster recovery plans, which are not explicitly required to be shared with relevant employees. In addition, the NAIC's Insurance Data Security Model Law currently includes the Cybersecurity Regulation's existing incident response plan requirements, but does not include any broader "operational resilience" requirements that are included in the Amendments.

D. CLASS A COMPANIES

The Amendments would create a new class of Covered Entities, designated as "Class A companies." A Covered Entity would be considered Class A if it has either:

1. "over 2,000 employees, including those of both the Covered Entity and all of its affiliates no matter where located"; or
2. "over $1,000,000,000 in gross annual revenue averaged over the last three fiscal years from all business operations of the Covered Entity and all of its affiliates."[17]

If a company meets the definition of a Class A company, then under the Amendments it would be obligated to implement additional cybersecurity monitoring and testing controls beyond those required of other Covered Entities. Among other controls, a Class A company would need to conduct an independent audit of its cybersecurity programs at least annually—a requirement that does not apply to other Covered Entities.[18] Class A companies would also be required to conduct weekly scans or reviews reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's information systems (whereas only "regular" reviews of this type would be required to be conducted by other Covered Entities).[19] Furthermore, at least once every three years, Class A companies would need to use external experts to conduct a risk assessment of cybersecurity risks to organizational operations, assets, stakeholders, and critical infrastructure stemming from the operation of an information system (as discussed below, other Covered Entities would be required to conduct risk assessments "periodically" and update them annually, with no requirement that external experts be used as part of this process).[20] And unless the Class A company's Chief Information Security Officer ("CISO") has approved reasonably equivalent controls in writing, the Amendments would require the Class A company to implement endpoint detection and response solutions to monitor anomalous activity, including but not limited to lateral movement, and a centralized solution for security event logging and alerting.[21] The latter requirement is not applicable to Covered Entities other than Class A companies.

E. WRITTEN CYBERSECURITY POLICIES

The proposed Amendments to Section 500.3 set forth new guidelines for what should be covered in a Covered Entity's written cybersecurity policies, including adding (as necessary) written policies to address "end of life management,"[22] remote access controls, and "vulnerability and patch management."[23] Furthermore, the amended Section 500.3 would require a Covered Entity's written cybersecurity policies to be approved by the Covered Entity's "senior governing body" (*i.e.*, generally, the Covered Entity's board of directors, an appropriate committee thereof, or an equivalent governing body)[24] at least annually, and implemented in accordance with documented procedures. Section 500.3 currently permits the written cybersecurity policies to be approved by a senior officer of the Covered Entity (which would not be permitted under the Amendments unless the Covered Entity does not have a board of directors or an equivalent governing body) and does not currently require that the written cybersecurity policies be approved annually.

Under the Amendments, a Covered Entity's written cybersecurity policies and procedures would also need to ensure a complete, accurate, and documented asset inventory, including all information systems and their components such as hardware, operating systems, applications, infrastructure devices, application program interfaces, and cloud services.[25] At minimum, these written policies would need to address the frequency with which a Covered Entity's asset inventory must be updated and validated, and the tracking of key information for each asset (including, as applicable, the owner, location, classification or sensitivities, support expiration date, and the recovery time requirements).[26]

A Covered Entity's written policies would also need to require encryption satisfying industry standards to protect nonpublic information held or transmitted by the Covered Entity.[27]

F. GOVERNANCE REQUIREMENTS

The Amendments would require that the Covered Entity's board of directors or an appropriate committee thereof have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cyber risk.[28] In addition, the board of directors or such committee would be required to establish a committee or subcommittee that would be assigned responsibility for cybersecurity.[29]

As described above, the Covered Entity's "senior governing body" would be required by the Amendments to approve the Covered Entity's written cybersecurity policies on at least an annual basis. In addition, if the Covered Entity has a board of directors, the Amendments would require the board or an appropriate committee thereof to direct executive management to develop, implement and maintain an information security program.[30] The Amendments would also require the Covered Entity's "senior governing body" to receive timely reports from a CISO with "adequate independence and authority to ensure cybersecurity risks are appropriately managed."[31] The CISO's reports to the senior governing body should address material cybersecurity issues, such as updates to the Covered Entity's risk assessment or major cyber events.[32] Finally, the Amendments would also require that any material gaps found during the testing of the cybersecurity program be documented and reported to both the Covered Entity's "senior governing body" and its senior management.[33]

G. ENHANCED ASSESSMENTS AND TESTING

As part of the Amendments, DFS would require that enhancements be made to existing testing and assessment regimes. For example, risk assessments would need to be updated at least annually under the Amendments, while the requirement under Section 500.9(a) that risk assessments be conducted "periodic[ally]" would remain in place.[34] A Covered Entity would also need to conduct an impact assessment whenever a change in the business or technology causes a material change to the Covered Entity's cyber risk.[35] The Amendments would also expand on the definition of a "risk assessment" to explicitly enumerate what constitutes a risk assessment. A risk assessment would be any "process of identifying cybersecurity

risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, customers, consumers, other organizations, and critical infrastructure resulting from the operation of an information system."[36] Under the Amendments, a risk assessment would need to take into account a Covered Entity's specific circumstances, 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."[37]

Penetration testing, already required to be conducted annually, would now be required to be conducted by a "qualified independent party."[38]

H. OTHER NEW REQUIREMENTS

The Amendments also include a number of prescriptive enhancements of existing required cybersecurity controls and implementation of new protective measures.

1. *Multi-factor authentication ("MFA")*. Under the Amendments, Covered Entities would be required to implement MFA for all remote access, third-party applications from which nonpublic information may be accessed, and privileged accounts (with certain exceptions).[39]
2. *Privileged Account Limitations*. Covered Entities would be required to limit both the number of privileged accounts and the access functions of those accounts to only those necessary to "perform the user's job," and review access privileges periodically to remove unnecessary access or accounts.[40] Class A companies would need to implement additional privileged account controls, including a "password vaulting solution for privileged accounts" and an automated method for blocking commonly used passwords.[41]
3. *Employee Training*. Covered Entities are already required to provide personnel with regular cybersecurity training, but the amended Cybersecurity Regulation would expand the cybersecurity awareness requirement to encompass, when appropriate, not only training but also exercises and simulations, and would also add the requirement that phishing training, exercises and simulations, when appropriate, be provided to all personnel.[42] Covered Entities would also be required to "monitor and filter emails to block malicious content from reaching authorized users."[43]

I. COMPLIANCE WITH AN AMENDED CYBERSECURITY REGULATION

Covered Entities would have 180 days to come into compliance with the Amendments following DFS's publication of a Notice of Adoption in the State Register. Section 500.22 provides for different compliance timelines for different amended provisions. A Covered Entity would have 30 days to comply with the updated notice requirements under amended Section 500.17. Separately, a Covered Entity would have one year to ensure strong, unique passwords are used,[44] and implement MFA for privileged accounts.[45] Additionally, Class A companies would have one year to implement endpoint detection and response solutions for monitoring anomalous activity and a solution for centralizing logging and security event alerting.[46]

Amended Section 500.20 now provides that the "commission of a single act prohibited" by the Cybersecurity Regulation constitutes a violation of the Regulation. The Amendments enumerate examples of an act that would constitute a single violation of the Cybersecurity Regulation, including failure to secure or prevent unauthorized access to nonpublic information due to noncompliance with any section of the Cybersecurity Regulation, or failure to comply with any section of the Cybersecurity Regulation for a 24-hour period.[47]

Also enumerated in the amended Section 500.20 are numerous considerations the Superintendent may take into account when assessing a penalty for a violation of the Cybersecurity Regulation, including the Covered Entity's cooperation with the Superintendent's investigation, the good faith of the Covered Entity, whether a violation was committed intentionally or as the result of failure to remedy previous examination matters requiring attention or failure to comply with DFS instructions, the Covered Entity's history of prior violations, the extent of customer harm, whether affected customers were provided accurate and timely disclosures, the gravity of the violations, the number of violations and length of time over which they occurred, the participation of any of the senior governing body in the violation, the Covered Entity's financial resources, net worth, and annual business volume, and "such other matters as justice and public interest require."[48]

J. EXEMPTIONS

Currently, Section 500.19 of the Cybersecurity Regulation exempts certain Covered Entities from provisions of the Cybersecurity Regulation. Currently, Covered Entities (including affiliates) with (i) fewer than 10 employees located in New York or responsible for business of the Covered Entity, (ii) less than $5,000,000 in average gross annual revenue over the last three years from New York business operations of the Covered Entity and its affiliates, or (iii) less than $10,000,000 in year-end total assets are exempted from certain Cybersecurity Regulation provisions, including staffing and testing requirements. The Amendments would expand the exemption to Covered Entities (including affiliates) with up to 20 employees or up to $15,000,000 in total year-end assets.[49]

IMPLICATIONS

The pre-proposed Amendments reflect DFS's continued efforts to elevate baseline industry cybersecurity standards to meet the challenges of the evolving cyber threat landscape. When initially passed in 2017, the Cybersecurity Regulation was a first-in-the-nation effort to impose prescriptive, baseline standards on banks and insurance companies. Several states followed suit, passing laws requiring baseline security standards that applied more broadly within their jurisdictions.

More recently, the federal government under the Biden Administration has taken unprecedented measures to impose prescriptive cybersecurity requirements intended to elevate security standards more broadly in the United States, including through the Executive Order on Improving the Nation's Cybersecurity, passed

last year and applicable to parts of the technology industry, and the Strengthening American Cybersecurity Act of 2022, which will require entities in the critical infrastructure sector report cyber incidents to CISA within 72 hours. Agencies under the Biden Administration have also enacted or proposed elevated reporting requirements that appear intended to heighten baseline security standards, including the SEC's currently proposed requirements that would substantially heighten required reporting on the nature of companies' cybersecurity governance and cybersecurity incidents they have experienced.

With federal and state regulators actively implementing and updating requirements and guidance in an effort to protect financial institutions and their customers from the harms associated with a cybersecurity event, financial institutions are in many cases subject to an ever-expanding patchwork of regulatory requirements, including as to both security measures that must be in place and notification requirements. The Cybersecurity Regulation and potential Amendments thereto make this especially true for banking organizations with operations in New York. Similarly, the Cybersecurity Regulation and potential Amendments, which apply to insurance organizations licensed in New York, are significantly more restrictive than the cybersecurity requirements provided for in the NAIC's Data Security Model Law.

The pre-proposed Amendments appear to reflect both the enhanced risk of ransomware attacks that has developed since the Cybersecurity Regulation was passed, and the increased regulatory focus on cybersecurity governance. The proposed requirement that a CISO have "sufficient independence and authority to manage cybersecurity risks" reflects a more recent, heightened regulatory focus in this area, including as reflected in the SEC's proposed cybersecurity rules, which would require companies to disclose to whom the CISO reports within the organization. Also significant is the proposed requirement that boards of directors obtain sufficient expertise and knowledge on cybersecurity risks, which has a corollary in the SEC's proposed rule requiring companies to disclose whether any member of the board has cybersecurity expertise. While boards in the banking and insurance industries have generally long addressed cybersecurity as part of their governance responsibilities, the fact that the DFS is underscoring that responsibility suggests there will be greater scrutiny of the role of the board of directors in the wake of a cybersecurity incident or failure to comply with the Cybersecurity Regulation.

Also noteworthy is DFS's effort to further tailor the Cybersecurity Regulation according to the size of a Covered Entity. While the current Cybersecurity Regulation exempts Covered Entities with relatively small employee headcounts and gross annual revenue from certain of the Cybersecurity Regulation's requirements, the Amendments would essentially create three "classes" of Covered Entities, each subject to varying cybersecurity requirements: (1) Class A companies with over 2,000 employees or over $1 billion in average gross annual revenue; (2) companies with between 2,000 and 20 employees or between $1 billion and $5 million in gross annual revenue; and (3) exempt companies with fewer than 20 employees, less than $5 million in gross annual revenue, and less than $15 million in total assets.

The proposed 24-hour extortion payment notification period appears to reflect a concern expressed by the U.S. government, most clearly since the Colonial Pipeline ransomware attack in 2021, that the government needs greater visibility into the nature and extent of the ransomware problem in the United States. It also aligns with the Strengthening American Cybersecurity Act of 2022, which will require companies in critical infrastructure sectors (a term to be defined more precisely for purposes of the law prior to implementation that is expected to include the financial services industry) to provide notification to CISA within 24 hours of a ransomware payment. The proposed Amendment to require a Covered Entity to evaluate alternatives before making such a payment, similar to a ransomware payment assessment requirement that has been proposed previously in Congress but not yet enacted, appears intended to make it less likely that a company will reflexively pay ransom under duress, consistent with the U.S. government's position that it discourages the payment of ransom.[50]

Covered Entities will have 180 days from the publication of any final version of these Amendments to bring their cybersecurity frameworks into compliance with the updated Cybersecurity Regulation (with the exception of certain specific requirements that are subject to different timelines, as described above).

* * *

ENDNOTES

1 23 NYCRR § 500.

2 A "Covered Entity" means any individual or non-governmental entity "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." 23 NYCRR at §§ 500.1(c), (i).

3 *Id.* at § 500.00.

4 Press Release, DFS, Department of Financial Services announces Cybersecurity Settlement with Mortgage Lender (Mar. 3, 2021), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202103031.

5 FED. RSRV., SR 22-4/CA 22-3: CONTACT INFORMATION IN RELATION TO COMPUTER-SECURITY INCIDENT NOTIFICATION REQUIREMENTS (2022), https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm.

6 OFF. OF THE COMPTROLLER OF THE CURRENCY, FED. RSRV., & FED. DEPOSIT INS. CORP., *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

7 According to the NAIC, as of July 8, 2022, the Insurance Data Security Model Law had been adopted in 21 jurisdictions. *See* NAIC, Implementation of Model Act #668 Insurance Data Security Model Law (status as of July 8, 2022), *available at* https://content.naic.org/sites/default/files/inline-files/Model%20%23668%20Map%20June%202022_0.pdf.

8 *See* Amendments at §§ 500.17(a)(3)-(4). *Cf.* Federal Rule at 70.

9 *See* Amendments at §§ 500.17(c)(1)-(2).

10 *See id.*

11 *See id.* at § 500.17(b).

12 *See id.* at §§ 500.17(b)(1)(i)(a)-(b).

13 *See id.* at §§ 500.17(b)(1)(ii)(a)-(c).

14 *See id.* at §§ 500.16(a)(1)(vi)-(vii), (d)(3), (e).

15 *See id.* at §§ 500.16(a)(2)(i)-(vi).

16 *See id.* at §§ 500.16(b)-(d).

17 *See id.* at § 500.1(c).

18 *See id.* at § 500.2(c). An independent audit would be defined as an "audit conducted by auditors free to make their decisions, not influenced by the [C]overed [E]ntities being audited or by its owners, managers, and employees." *Id.* at § 500.1(f). An independent audit could be "conducted by auditors internal or external to the [C]overed [E]ntity and its affiliates." *Id.*

19 *See id.* at § 500.5(a)(2).

20 *See id.* at § 500.9(d).

21 *See id.* at §§ 500.14(b)(1)-(2).

22 In general, the term "end of life management" refers to managing the use of a product or system after its original manufacturer or provider has stopped producing, supporting or providing upgrades for it.

ENDNOTES (CONTINUED)

23 *See id.* at §§ 500.3(c), (d), (o).

24 In circumstances where a Covered Entity does not have a board of directors or an equivalent governing body, the senior officer of the Covered Entity responsible for the Covered Entity's cybersecurity program would be considered the "senior governing body" of the Covered Entity.

25 *See id.* at § 500.13(a).

26 *See id.* at §§ 500.13(a)(1)-(2).

27 *See id.* at § 500.15(a). The Amendments maintain an exception for Covered Entities for whom encryption is infeasible, while placing additional responsibilities on the CISO to ensure the effectiveness of these controls, though the CISO would need to review and approve of these alternative compensating controls in writing. *See id.* at § 500.15(b).

28 *See id.* at § 500.4(d).

29 *See id.*

30 *See id.*

31 *See id.* at §§ 500.4(a), (c).

32 *See id.* at § 500.4(c).

33 *See id.* at § 500.5(b).

34 *See id.* at § 500.9(c); 23 NYCRR § 500.9(a).

35 *See* Amendments at § 500.9(c).

36 *See id.* at § 500.1(n).

37 *Id.*

38 *See id.* at § 500.5(a)(1).

39 *See id.* at § 500.12(b). MFA would not be required for privileged service accounts that prohibit interactive login and for which a CISO has approved in writing of the implementation of compensating controls that achieve reasonably equivalent security. *See id.* at §§ 500.12(c)(1)-(2).

40 *See id.* at §§ 500.7(a)(2), (4).

41 *See id.* at § 500.7(b)(1)-(2).

42 *See id.* at § 500.14(a)(3).

43 *See id.* at § 500.14(a)(2).

44 *See id.* at § 500.7(b).

45 *See id.* at § 500.12(c).

46 *See id.* at § 500.14(b).

47 *See id.* at § 500.20(b)(1)-(2).

48 *See id.* at § 500.20(c)(1)-(15).

49 *See id.* at § 500.19(a)(1), (3).

50 *See* U.S. SENATE COMM. ON HOMELAND SEC. AND GOVERNMENTAL AFFS., *Peters and Portman Introduce Bipartisan Legislation Requiring Critical Infrastructure Entities to Report Cyber-Attacks* (2021), https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks; Tim Starks, *Cyber Incident Reporting Mandates Suffer Another Congressional Setback*, CYBERSCOOP.COM

ENDNOTES (CONTINUED)

(Dec. 7, 2021), https://www.cyberscoop.com/cyber-incident-reporting-ransomware-payments-congress-ndaa/.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.