Assessment of Public Comments on the Revised Proposed Second Amendment to 23 NYCRR Part 500

The New York State Department of Financial Services ("Department" or "DFS") received comments from banking, insurance, and other industry groups, regulated organizations, unregulated businesses, and members of a law school law society regarding the Second Amendment to 23 NYCRR Part 500 (the "Cybersecurity Regulation").

Commenters made comments that were previously submitted and that DFS addressed in its initial assessment of public comments, which were published in the State Register on June 28, 2023 (the "Assessment"). See the Assessment for detailed responses to those comments. DFS received the following new comments.

Commenters stated their support for the following changes in the Cybersecurity Regulation: (1) providing clarification that only those affiliates sharing information systems, cybersecurity resources, or all or any part of a cybersecurity program with a covered entity should be included when calculating the number of employees and gross annual revenue in the definition of "class A companies"; (2) including audits conducted by internal auditors in the definition of "independent audit"; (3) removing accounts that can affect a material change to the technical or business operations of the covered entity from the definition of "privileged account"; (4) removing the requirement that the senior governing body "provide direction to management" on a covered entity's cybersecurity risk management in § 500.4(d); (5) replacing the senior governing body's obligation to have "sufficient expertise and knowledge" with the obligation instead to have "sufficient understanding" of cybersecurity-related matters in § 500.4(d); (6) removing the requirement for class A companies to use external experts to conduct a risk assessment at least once every three years in § 500.9; (7) clarifying that the privileged accounts for which limited exempt entities must use multi-factor authentication ("MFA") in § 500.12(a)(3) do not include "service accounts that prohibit interactive login"; (8) adding requirements for class A companies to implement endpoint detection and response solutions and solutions that centralize logging in § 500.14; (9) clarifying that covered entities only need to establish the requisite incident response and business continuity and

disaster recovery ("BCDR") plans in § 500.16(a) for "cybersecurity events" and not all "disruptive events;" (10) clarifying that covered entities can submit their certification of compliance required by § 500.17(b) as long as they "materially complied with" the requirements of Part 500 "during the prior calendar year;" and (11) adding the requirement that a failure to comply for any 24-hour period with any section of Part 500 must be material to constitute a violation in § 500.20(b)(2).

Comment: Commenters generally requested that the Department: (1) continue to take a risk-based approach to cybersecurity; (2) align Part 500 with other cybersecurity rules and frameworks, such as the cybersecurity rules promulgated by the U.S. Securities and Exchange Commission ("SEC") and the frameworks published by the National Institute of Standards and Technology ("NIST"), including the draft NIST Cybersecurity Framework 2.0 ("NIST CSF 2.0"); (3) increase collaboration between the Department and its regulated entities; and (4) describe how covered entities can meet their responsibilities under Part 500, recommend additional cybersecurity steps they can take, and include reference points of a "mature" program.

Response: DFS's Cybersecurity Regulation takes a risk and principles-based approach because it applies to the broad scope of financial services organizations DFS regulates, which includes companies of very different sizes with different business models in various industries, such as banking and insurance. DFS is not changing this general approach.

Throughout the drafting and notice and comment periods, the Department reviewed other cybersecurity regulations and frameworks currently in effect, including those of the SEC and NIST, as well as proposed laws and regulations from other states, the federal government, and other countries. Where relevant and appropriate given its mission, the Department harmonized its requirements with other regulations and frameworks. For example, the Cybersecurity Regulation emphasizes governance controls in alignment with NIST CSF 2.0.

The Department looks forward to continuing its tradition of collaboration with industry to promote understanding of cybersecurity generally and compliance with Part 500 specifically. The Department maintains

detailed information regarding compliance with Part 500 on its website in the Cybersecurity Resource Center, which the Department updates regularly.

Therefore, the Department did not make any changes in response to these comments.

Comment: Commenters requested that DFS add a definition of "deployment" because it is used in § 500.17(a) when specifying the notification requirement regarding ransomware.

Response: The Department declines to add a definition of "deployment" because deployment is a commonly understood term and the dictionary definition is intended.

Comment: A comment suggested DFS include a new section to address the cybersecurity risks associated with artificial intelligence ("AI"), generative AI, and large language models.

Response: The Department agrees that cybersecurity risks associated with AI are concerning, and therefore expects covered entities to take these risks into account in their risk assessments and address them in their cybersecurity programs. The Department will continue to monitor emerging issues involving AI, generative AI, and large language models and assess whether to adopt future amendments to the Cybersecurity Regulation. However, the Department declines to add a new section regarding AI and large language models at this time.

Comment: Commenters requested that DFS delete the part of the proposed definition of "Chief Information Security Officer or CISO" that requires that a CISO have "adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain an effective cybersecurity program," because CISOs do not typically make enterprise-wide resource allocation or other decisions. Rather, resource allocation decisions are typically the responsibility of the CEO or similar senior management. Commenters further noted that such requirements do not align with industry governance and operational practice, thereby creating an unworkable obligation for CISOs.

Response: DFS understands that CISOs typically do not have the ability to allocate a company's budget and other resources; rather, senior management, governed by the board, generally has that authority. Accordingly, the

Department clarified that it is the senior governing body's duty to confirm "that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program" by adding such language to § 500.4(d) and removing "who has adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources needed to implement and maintain an effective cybersecurity program" from the definition of "Chief Information Officer or CISO."

Comment: Commenters requested that the Department revise the definition of "class A companies" to exclude, among other things, affiliates that share, only in a limited capacity, information systems, cybersecurity resources, or a cybersecurity program with the covered entity and are largely separate, such as financial institution groups where the only covered entity within the group is a "representative office."

Response: The Department recognizes that cybersecurity is a complex issue and that cybersecurity programs must be tailored to the risks and assets of each covered entity. Where a covered entity is part of a larger group that shares information systems, cybersecurity resources or any part of a cybersecurity program, focusing solely on the size of the covered entity would ignore the larger risk to which the covered entity is subject. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that the Department revise the definition of "covered entity" by, among other things, specifically excluding federally-regulated institutions that maintain a DFS license for a specific activity. One commenter requested that the Department clarify whether managed care organizations regulated by the New York State Department of Health ("NYSDOH"), such as Article 44 health maintenance organizations ("HMOs"), are subject to Part 500 because according to this commenter, the added language "regardless of whether the covered entity is also regulated by other government agencies" in § 500.1(e) appeared to be an attempt to encompass plans primarily regulated by NYSDOH.

Response: Federally-regulated institutions that apply for, and are granted, a license to perform a service that is regulated by DFS must comply with the regulations that apply to anyone who holds such a license, including

Part 500. The clause "regardless of whether the covered entity is also regulated by other government agencies" was added to the definition of "covered entity" in § 500.1(e) to clarify that Part 500 applies to entities that qualify as covered entities, regardless of whether they are also regulated by another government agency.

Only certain entities regulated by the NYSDOH are subject to DFS authority and are considered "covered entities" and, absent an exemption pursuant to § 500.19, must comply with the requirements of Part 500, namely those entities operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, Insurance Law or Financial Services Law. For example, DFS has previously addressed questions regarding the applicability of Part 500 to Article 44 HMOs, stating in the Department's Cybersecurity Resource Center that Article 44 HMOs are covered entities because pursuant to the Public Health Law, HMOs must receive authorization and prior approval for the forms they use and the rates they charge for comprehensive health insurance in New York, and furthermore, the Public Health Law subjects HMOs to DFS authority through applicable provisions of the Insurance Law. As this authorization is fundamental to the ability to conduct their businesses, HMOs are covered entities because they are "operating under or required to operate under" DFS authorizations pursuant to the Insurance Law. With respect to Article 44 managed care organizations, DFS requires all entities whose certificate of authority indicates that it is an HMO to comply with Part 500, including Medicare Advantage HMOs, but DFS has not required Managed Long Term Care Plans or Prepaid Health Service Plans to comply.

Therefore, the Department did not make any changes in light of these comments.

Comment: Although the Department did not propose any changes to the definition of "cybersecurity event," commenters requested that the Department revise the definition to align with other rules, laws, and regulations by: (1) adding the terms "unintentional, non-malicious acts" and "confidentiality, integrity and availability;" and (2) removing "unsuccessful attempts" because it is not possible to report all unsuccessful attempts.

Response: The Department endeavors to harmonize and align with other rules, laws, and regulations, doing so where appropriate and practical for DFS-regulated entities and where it aligns with DFS's mission. Section 500.17(a) requires notification to the Department of certain cybersecurity events, such as those that have a reasonable likelihood of materially harming any material part of the normal operations of a covered entity or where notice is required to be provided to another governmental body. The Department believes that the suggested modifications are unnecessary because the definition of cybersecurity event properly captures the type of event the Department intends to include in the Cybersecurity Regulation. The Department views the terms "unauthorized access," "disrupt," and "misuse" as used in the definition of cybersecurity event as equivalent in meaning to the terms "confidentiality, integrity and availability." As stated on the Department's website in the Cybersecurity Resource Center, the Department recognizes that covered entities are regularly subject to many attempts to gain unauthorized access to, disrupt or misuse information systems and the information stored on them, and that many of these attempts are thwarted by the covered entities' cybersecurity programs. It is these types of events, and not unintentional or non-malicious actions, that are the focus of the Cybersecurity Regulation. Finally, the Department anticipates that most unsuccessful attacks will not be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the covered entity, are sufficiently serious to raise a concern. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that DFS use the term "cybersecurity incident" instead of "cybersecurity event" to align with the term's use in other rules, laws, and regulations.

Response: In light of this comment and the Department's understanding of the current typical industry usage of the term "cybersecurity incident," the Department is adding "cybersecurity incident" as a defined term in the Cybersecurity Regulation by moving language that had been embedded in § 500.17(a)'s requirement to report cybersecurity events. Thus, although the defined term "cybersecurity incident" is new, the text in the definition

itself, for the most part, is not, and the substantive reporting requirements remain. The Department is retaining the term "cybersecurity event" because it is used in other provisions of Part 500 besides § 500.17.

Comment: One commenter requested that the Department describe the processes and procedures for conducting internal audits that would comply with Part 500.

Response: The processes and procedures a covered entity should use when conducting internal audits depend upon the specific circumstances of that entity and the particular risks it faces. Describing such processes and procedures in the regulation is contrary to Part 500's flexible, risk-based approach. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department revise the definition of "information system" in § 500.1 by adding to the end of this definition "systems that contain customer information or that are connected to a system that contains customer information" because § 500.12 generally requires MFA for any individual accessing any "information system" and MFA is unnecessary where there is no risk of access to non-public information.

Response: Many information systems that do not themselves contain or connect to systems that contain customer information, such as firewalls, routers, switches and VPN appliances, could be compromised, and if they are, those systems could be leveraged to bypass cybersecurity controls and compromise information systems that contain nonpublic information or jeopardize the covered entity's ability to provide financial services. Therefore, the Department declines to make any changes in light of this comment.

Comment: One commenter requested that the Department add examples to the definition of MFA and stated that it is onerous to require physical tokens.

Response: The Department declines to add specific examples of MFA because specific examples could quickly become obsolete. Furthermore, when defining MFA, DFS did not mandate the use of any specific type of MFA, including the use of physical tokens, because a covered entity should decide what type of MFA to

implement based on its risk assessment. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department broaden the definition of "penetration testing" in § 500.1 by specifying that the covered entity authorize the testing and explicitly adding a requirement that a covered entity conduct testing on databases and controls.

Response: The Department is clarifying this definition to provide that the covered entity authorize the penetration testing. However, the Department does not believe the other requested change is necessary because the scope of a covered entity's penetration testing must be determined by its risk assessment. Therefore, the Department added the word "authorizing" prior to "attempted penetration" in light of this comment.

Comment: One commenter requested that the Department use the NIST definition of "privileged account" or delete the language "more or less secure" at the end of the definition of "privileged account" in § 500.1 because it is superfluous.

Response: The Department based its definition on NIST's definitions of "privileged user" and "privileged account," and agrees that the language "to make them more or less secure" is unnecessary as it does not add anything to the definition. Therefore, the Department is deleting that language in light of this comment.

Comment: One commenter requested the Department reinsert language in the definition of "risk assessment" that describes what such assessments should take into account (i.e. 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), because it helps covered entities understand DFS's expectation that a risk assessment must be based on their specific circumstances.

Response: The Department declines to make any change at this point as the definition of "risk assessment" aligns with industry definitions and standards.

Comment: One commenter requested that the Department revise the definition of "senior officer(s)" in §500.1 to include senior officer(s) of an affiliate when a covered entity adopts all or part of a cybersecurity program from that affiliate pursuant to § 500.2(d).

Response: The definition of "senior officer(s)" is not restricted to employees of a covered entity, and includes "the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a covered entity[.]" To the extent these individuals are employed by an affiliate and perform the functions referenced in this definition on behalf of the covered entity, they would be considered senior officers of the covered entity. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that the Department revise the definition of "third-party service provider" to: (1) provide examples of what DFS means by "governmental entity"; (2) add specific examples of what would not be considered a third-party service provider; and (3) add that a third-party service provider must have a contractual relationship with the covered entity.

Response: The Department declines to add the requested examples because these additions are too granular and may result in Part 500 becoming outdated quickly. The Department will consider providing examples in guidance. The Department also declines to require a contractual arrangement in the definition because DFS does not want to exclude covered entities that do not currently have contractual arrangements with their third-party service providers from the requirements in § 500.11 regarding third-party service provider security policies or encourage covered entities to avoid contractual relationships to avoid those requirements. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that the Department add a new subsection to § 500.2 (Cybersecurity Program) that would require covered entities to establish reasonable administrative, technical and physical

practices that take into account the specific nature of their businesses, such as the volume and nature of nonpublic information maintained, their organizational and operational requirements, and the risks they face.

Response: Section 500.2(b) already requires covered entities to base their cybersecurity programs on their risk assessments, which take into account the specific nature of their businesses and the particular risks they face. The Department expects covered entities to establish administrative, technical, and physical cybersecurity controls that are reasonable based on those specifics and the risks identified in their risk assessments. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters recommended that DFS change the frequency of the annual audit requirement for class A companies required in § 500.2(c) because the audit requirement is, among other things, burdensome, onerous and time-consuming. Specifically, commenters recommended that DFS only require an audit when there is a material change in a covered entity's business or technology, or at a frequency based on the results of their risk assessment. Commenters also requested that DFS clarify the requisite scope of the audit required for class A companies because their ability to conduct comprehensive cybersecurity audits each year is unrealistic due to the complexity of their cybersecurity programs.

Response: In response to the comments received and as a result of the Department's understanding that class A companies typically conduct more than one audit each year on the companies' cybersecurity programs, the Department is clarifying § 500.2(c) by replacing the annual audit requirement with a requirement to conduct audits at a frequency that is based on a class A company's risk, and specifying that class A companies must design, as well as conduct, the audit.

Comment: One commenter requested that the Department revise § 500.2(d), which permits covered entities to adopt all or part of an affiliate's cybersecurity program as long as the adopted portions or program comply with Part 500, to deem covered entities to be compliant if they have obtained certifications of compliance with a

cybersecurity standard containing requirements comparable to those in Part 500, such as ISO/IEC 27001 from the International Organization for Standardization.

Response: Certifications demonstrating compliance with a different cybersecurity standard do not guarantee compliance with all requirements of Part 500. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that, in § 500.3, DFS restore the ability of a senior officer to approve a covered entity's cybersecurity policy or policies because senior management has the technical expertise and daily involvement necessary to approve such policies. In addition, commenters requested that DFS: (1) allow the CISO to approve the cybersecurity policy or policies; (2) only require approval when there are material changes to the policy or policies; and (3) emphasize that oversight includes appropriate review and understanding of the covered entity's cybersecurity policies.

Response: In response to these comments, the Department is restoring the ability of a senior officer to approve a covered entity's cybersecurity policy or policies. The Department believes that it is important for a senior officer or the senior governing body to approve the policies annually even when there are no material changes because in order to approve, the senior officer or senior governing body must review the policies to determine that there have been no material changes, and this review process is important. Regardless of whether a senior officer or the senior governing body approves a covered entity's cybersecurity policies, § 500.4(d) requires that the senior governing body have sufficient understanding of the substance of the cybersecurity policies to exercise oversight of a covered entity's cybersecurity program.

Comment: One commenter requested that the Department revise § 500.4(a) to only require class A companies to designate a CISO.

Response: The Department declines to require the designation of a CISO only for class A companies. Most covered entities will not qualify as class A companies but still need a CISO. Part 500 remains flexible in this

regard by allowing the CISO to be employed by a third-party service provider or an affiliate. Furthermore, smaller covered entities that qualify for a limited exemption pursuant to § 500.19(a) are not required to have a CISO, although depending on their risk assessment, such entities may also designate a CISO.

Comment: Commenters requested that the Department: (1) clarify what the requisite annual report from the CISO to the senior governing body should include when it refers to "plans for remediating material inadequacies" in § 500.4(b); and (2) add after "plans for remediating material inadequacies" the language "generated by responsible persons" to ensure that the CISO's report includes only plans created by staff who are responsible for their information systems.

Response: The Department declines to clarify what is meant by material inadequacies because what constitutes material inadequacies will vary for each covered entity and will depend on their specific circumstances, although it may include areas of noncompliance with Part 500 or other cybersecurity laws and regulations as well as unacceptable cybersecurity risks. The Department also declines to add "generated by responsible persons" because it is commonly understood that a covered entity should only rely on plans for remediating material inadequacies that are generated by responsible persons. Therefore, the Department is not making any changes in light of these comments.

Comment: One commenter recommended that the Department allow the CISO to timely report to a senior officer in addition to the senior governing body on material cybersecurity issues as required by § 500.4(c) because requiring CISOs to report such issues directly to the senior governing body does not provide covered entities with sufficient flexibility in determining their corporate reporting structure or align with typical industry governance and operational practices. One commenter requested that the Department clarify § 500.4(c) to allow vulnerability testing readouts to be reviewed by executives overseeing vulnerability management, rather than the board.

Response: To provide covered entities with flexibility to design and implement effective governance approaches that align with industry governance and operational practices, the Department is clarifying § 500.4(c)

to require the CISO to timely report either to the senior governing body or senior officer(s) on material cybersecurity issues. If a regulated entity chooses to have its CISO report material issues to senior officers instead of the senior governing body, the Department expects the senior officers to whom the report was made to take appropriate actions in response to the report, including by escalating any relevant issues to the senior governing body.

Part 500 does not contain specific requirements regarding vulnerability testing readouts and, therefore, the Department is not making any changes in light of this request for clarification.

Comment: One commenter asked the Department whether a senior officer of a DFS-licensed subsidiary of a holding company could fulfill the requirements required of a senior governing body if the subsidiary does not have a board of directors.

Response: The requirements in § 500.4(d) apply to the senior governing body, which can be "the senior officer or officers of a covered entity responsible for the covered entity's cybersecurity program" when the covered entity does not have a board of directors or equivalent governing body. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter recommended that DFS revise the language in § 500.4(d) to clarify that the senior governing body does not have to oversee the details of the cybersecurity program and that executive management may be in charge of such oversight because covered entities need flexibility to determine how best to ensure such oversight is effective.

Response: The Department believes that the oversight role of a senior governing body differs from the direct management role played by senior management, and that such difference is well established in law and industry practice. The amendment does not require the senior governing body to be responsible for the details of the cybersecurity program; such responsibility rests with executive management or its designees pursuant to §500.4(d), which requires the senior governing body to require that "the covered entity's executive management

or its designees . . . develop, implement and maintain the covered entity's cybersecurity program." Therefore, the Department did not make changes in light of this comment.

Comment: One commenter requested that the Department remove the requirement that the senior governing body have "sufficient understanding" of cybersecurity-related matters in § 500.4(d) because the CISO has such understanding and reports to the senior governing body. Another commenter requested that DFS clarify the meaning of "sufficient understanding" because it is "vague."

Response: A board of directors must have a sufficient understanding of the risks that apply to their organization to effectively perform its oversight function in compliance with applicable laws and regulations. Accordingly, the senior governing body must understand cybersecurity-related matters enough to exercise effective oversight of cybersecurity risk management and question management about their cybersecurity program and significant cybersecurity events impacting the covered entity, among other things. Whether a governing body has "sufficient understanding" depends on the particular circumstances of the covered entity and the specific cybersecurity program of that entity. Therefore, the Department declines to make changes in light of this comment.

Comment: One commenter requested that the Department change the title of § 500.5 from "Vulnerability management" back to "Vulnerability assessments."

Response: Section 500.5 contains requirements with respect to penetration testing, monitoring, and remediation, which are more accurately encompassed within the term vulnerability management. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that the Department remove the term "manual" from the requirement to perform manual reviews of systems not covered by automated vulnerability scans in § 500.5(a)(2) since a manual review is a specific method of review that is unnecessarily limiting because there may be other automation beyond scanners that would be more appropriate.

Response: The requirement for a manual review requires human involvement to the extent automated scans cannot scan or reach systems that need scanning; it does not require a manual inspection. When automated scans cannot reach or do not cover particular systems, those systems must be manually reviewed with human involvement, and the individual performing such review may use any appropriate tools available to facilitate the manual review. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that the Department remove "timely" with respect to the requirement to remediate vulnerabilities in § 500.5(c) because it is subjective and covered entities need flexibility to remediate vulnerabilities in accordance with the risks they pose.

Response: Based on the Department's experience and the broader reporting and discussion relating to publicly reported cyberattacks, there is no doubt that vulnerabilities must be remediated in a "timely" manner. Nonetheless the amendment provides covered entities with flexibility by not defining a specific time frame within which vulnerabilities must be remediated. Accordingly, "timely" remediation should be assessed within the context of a number of factors, including the seriousness of the vulnerability, the work required to remediate the vulnerability, and the remediation cadence. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that the Department clarify the term "account" as it is used in §500.7(a) with respect to access privileges and management requirements.

Response: The Department did not make any changes in light of this comment because the definition of account is commonly understood in the industry as a means by which a user is permitted access to an information system.

Comment: One commenter stated that the requirements in §500.7(a)(4) to review all user access privileges and remove or disable accounts and access that are no longer necessary are too broad in application, especially as they relate to third-parties, vendors, and customers.

Response: Cyberattacks are often successful due to poor user access controls, including a failure to review and remove accounts and privileges that are no longer used or needed. To limit the risk of a malicious actor using old account credentials, the amendment requires covered entities to review all user access privileges to ensure that every user has only the access privileges that such user needs and no more. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that the Department revise the requirement in § 500.7(a)(5) to disable or securely configure all protocols that permit remote control of devices by adding language that a covered entity must "take reasonable measures, based on the risk assessment" when fulfilling such requirement.

Response: Since all measures taken by a covered entity must be based on its risk assessment and must be reasonable given the risks of the covered entity, the Department declines to make any changes in light of this comment.

Comment: Commenters requested that the Department modify the requirements for class A companies to monitor privileged access activity and implement the two specified controls required in § 500.7(c) by allowing covered entities to determine what monitoring and other controls to implement based on their risk assessments. Other commenters requested that the Department: (1) remove the words "shall monitor privileged activity" because it is not clear whether covered entities must use a technological solution when monitoring; (2) change the word "monitor" to "log" because the word "monitor" implies "more active conduct" and covered entities should be permitted to perform active monitoring based on their risk assessments; and (3) clarify what is meant by the term "solution."

Response: Although Part 500's approach generally is not prescriptive, to ensure covered entities implement cybersecurity programs that match their risk profile the Department believes monitoring privileged access activity is a regulatory minimum standard and control warranted for class A companies in light of the cybersecurity threat landscape. That said, class A companies have the flexibility and discretion to determine how such monitoring

should be implemented, including whether to use a technological solution. Moreover, the term "solution" is commonly understood in cybersecurity management and can be a hardware or software product or service or combination thereof. Furthermore, the Department declines to make the change from "monitor" to "log" because the Department believes that monitoring, which requires active conduct, is critical for detecting anomalous activity, and covered entities must determine, in accordance with the risk assessment, which activity to monitor. Therefore, the Department did not make changes in light of these comments.

Comment: Commenters recommended that DFS: (1) remove the requirement in § 500.7(c)(2) for class A companies to implement an automated method of blocking commonly used passwords; (2) exclude accounts not owned by a class A company; (3) define "controlled" and "commonly used password"; (4) include "to the extent passwords are employed as a method of authentication" to be consistent with § 500.7(b); and (5) change the word "automated" to "systematic" to allow for manual processes.

Response: An automated password blocking solution is an important measure used to ensure compliance with written password policies and the Department believes it is a regulatory minimum standard and control warranted for class A companies in light of the cybersecurity threat landscape. In certain situations where implementing this solution is infeasible, the CISO may approve reasonably equivalent or more secure compensating controls. The Department does not believe it appropriate to base this requirement on account ownership instead of ownership or control of information systems. Also, the Department does not believe it necessary to further specify that this requirement only applies when passwords are used because the requirement in this provision is to implement the automated solution to block commonly used passwords, and it is implicit that this solution could only apply to password protected accounts. In addition, the terms "controlled" and "commonly used passwords" are widely understood in the industry. Lastly, the Department believes that automated solutions are preferable and does not want to allow for manual processes.

Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that DFS revise § 500.7(c)(2) to: (1) allow class A companies to implement controls other than automated methods of blocking commonly used passwords, such as increasing password complexity; or (2) require the implementation of such controls based on risk assessments that may indicate the need for such controls only for privileged accounts and not for all accounts. One commenter requested more guidance on measures DFS considers "reasonably equivalent or more secure."

Response: Implementation of an automated method of blocking commonly used passwords is important for securing access to all password protected accounts, not only privileged accounts, and the Department believes this control is a requisite minimum standard control for all class A company accounts, and not just for privileged accounts, in light of the cybersecurity threat landscape. Increasing password complexity does not yield the same results.

Determining what constitutes "reasonably equivalent or more secure" compensating controls should be based on the specific circumstances of the class A company and its risk assessment.

Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that the Department revise the application security requirements in §500.8 to require that organizations anonymize nonpublic information that is used during application development and testing.

Response: While the Department appreciates the commenter's suggestions and agrees that anonymizing nonpublic information that is used during application development and testing may be beneficial to a covered entity's cybersecurity program, the Department declines to add such a prescriptive requirement at this time. Rather, as part of general risk-based approach taken by the Cybersecurity Regulation, anonymizing nonpublic information is a control that covered entities should consider and implement if appropriate given the risk profile and resources of the covered entity.

Comment: Commenters requested that the Department clarify the risk assessment requirements in § 500.9 because, among other things, it was unclear how to read subsections (a) and (c) together.

Response: In light of these comments, the Department made a clarifying change to § 500.9 by deleting §500.9(c), which required the risk assessment to be reviewed and updated at least annually and whenever a change in the business or technology causes a material change to the covered entity's cyber risk, and incorporated the substance of this requirement into the text of § 500.9(a). The Department further deleted text in § 500.9(a) in order to clarify that the risk assessment must be reviewed and updated as reasonably necessary, but at least annually, and "whenever a change in the business or technology causes a material change to the covered entity's cyber risk."

Comment: One commenter recommended that the Department remove the requirement for verifying that key cybersecurity personnel maintain knowledge of cybersecurity threats and countermeasures in § 500.10(a)(3) because the term "key cybersecurity personnel" is vague.

Response: Key cybersecurity personnel are those essential individuals responsible for implementing and monitoring a covered entity's cybersecurity program. In light of the cybersecurity threat landscape, it is important that these individuals maintain their knowledge of cybersecurity threats and countermeasures. Therefore, the Department did not make any changes in response to this comment.

Comment: Commenters requested that the Department provide examples of third-party risks in § 500.11, such as "supplier failure, service deterioration, and concentration risk," to encourage covered entities to use mitigation strategies, and provide guidance relating to third-party due diligence and assessments.

Response: Although the Department appreciates the commenters' suggestions, it believes Part 500 already encourages mitigation strategies and did not make any changes in response to these comments; however, the Department is considering providing guidance on § 500.11 and third-party risks.

Comment: One commenter requested that the Department specifically exclude authorized insurers and licensed producers from the requirement to conduct due diligence on each other in § 500.11 because it serves little public purpose for a producer to conduct due diligence on a multi-billion-dollar insurer and because an insurer is unlikely to give agency appointments to agencies they have not investigated prior to appointment.

Response: Section 500.11 has never contained any specific exclusions, and the Department declines to add any at this time. This provision requires each covered entity to implement risk-based third-party service provider policies and procedures that address certain topics to the extent applicable, including due diligence. The Department recognizes that, in certain cases, a covered entity that seeks to contract with a third party, whether or not that third party itself is a covered entity, may have limited ability to perform due diligence or to require contractual terms regarding cybersecurity. For example, larger third-party service providers make available standard due diligence information and may refuse to complete individual questionnaires or otherwise make information available. This is most common where the covered entity is small and the third-party service provider is significantly larger, resulting in limited due diligence opportunities and contractual terms that are often one-sided in favor of the third-party service provider. In such situations, a covered entity must still review available information and any contractual agreements and only transact with the third-party service provider if the covered entity is otherwise comfortable that the relationship satisfies the covered entity's risk tolerance, including with respect to any cybersecurity risk.

With respect to insurance companies, the Department expects as part of their investigation of the agents they appoint, that the insurance company is comfortable with the results of such investigations, including with respect to any associated cybersecurity risk, and the insurance company's policies and procedures should reflect its investigation and due diligence practices, in accordance with § 500.11.

Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that DFS clarify whether MFA is required in a variety of fact patterns, such as when users access a covered entity's: (1) internal information systems from the covered entity's office; or (2) internal or external information systems from their mobile devices if the mobile device had specific software, hardware, certificates, or possession tokens.

Response: Section 500.12(a) requires MFA to be used for any individual accessing any information systems of a covered entity, regardless of location, type of user, and type of information contained on the information system being accessed, with few exceptions. It may be acceptable, in some circumstances, depending on a covered entity's specific cybersecurity risks, to use a device, such as an office workstation, mobile phone, or laptop, as one of the authentication factors required for MFA, especially if, for example, the device contains biometric capabilities or authenticator applications.

Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that DFS clarify whether a possession factor and either a knowledge factor or an inherence factor would satisfy the MFA requirements in § 500.12.

Response: Section 500.1(i) already defines MFA to mean authentication through verification of at least two of the three types of authentication factors listed, which are knowledge, possession, and inherence factors. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that DFS clarify whether MFA is required when: (1) users are not accessing information systems that contain nonpublic information; (2) a user accesses a public facing website; or (3) a customer logs into a covered entity's online portal.

Response: Pursuant to § 500.12, covered entities must require users to provide multiple forms of authorization to access any of the covered entity's information systems, regardless of the type of information maintained on such systems. MFA generally is not required for visits to a covered entity's public facing website because visits to public facing websites do not require access to a covered entity's information systems. However,

if a customer logs into a covered entity's online portal from a public facing website, that customer would be accessing the covered entity's information systems and must use MFA. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters stated that the MFA requirements in § 500.12 may exceed the Department's jurisdiction and cause conflicts with the Federal Trade Commission's Safeguards Rule (the "FTC Safeguards Rule") and other state and federal requirements.

Response: The MFA requirements in § 500.12 are well within DFS's authority under the Financial Services, Banking, and Insurance Laws and align with those in the FTC Safeguards Rule. As stated above, the Department has endeavored to align all requirements in Part 500 with those in other laws and regulations as much as possible when the mandates of, and entities regulated by, DFS and the other regulators overlap. Therefore, DFS did not make any changes in response to this comment.

Comment: Commenters recommended that the MFA requirements be based on a risk assessment because authentication measures should correspond to the value and sensitivity of the assets or information involved and the MFA requirements in § 500.12 are therefore overly prescriptive and inefficient.

Response: MFA is a regulatory minimum standard and control that is required for any individual accessing a covered entity's information systems because, based on cybersecurity events that have been reported to DFS and those events that are publicly known, authentication weaknesses are the most common cybersecurity gap exploited by cyber threat actors at financial services companies. MFA has proven to be one of the most effective and inexpensive ways to reduce this risk. The amendment provides covered entities with flexibility to deem MFA unnecessary for access to certain information systems under certain circumstances if the covered entity has a CISO and that CISO has approved in writing the use of reasonably equivalent or more secure compensating controls. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that DFS clarify § 500.12(a) by rephrasing the requirement for "any individual accessing any of the covered entity's information systems" to state instead "any individual accessing any information of a covered entity."

Response: In response to this comment, the Department is clarifying the language in § 500.12(a) by changing "any individual accessing any of the covered entity's information systems" to "any individual accessing any information systems of a covered entity." This change also more closely aligns the Cybersecurity Regulation with the FTC Safeguards Rule.

Comment: One commenter requested that the Department remove the phrase "[I]f the covered entity has a CISO" at the beginning of § 500.12(b) because it is unnecessary as all covered entities must have a CISO pursuant to § 500.4(a). Another commenter requested that DFS state clearly that the CISO may approve alternative controls in § 500.12.

Response: Covered entities that qualify for the limited exemption in § 500.19(a) are not required to have a CISO because they are exempt from the requirements in § 500.4. If a covered entity does not have a CISO, it cannot avail itself of the potential use of reasonably equivalent or more secure compensating controls pursuant to § 500.12(b). Further, § 500.12(b) explicitly states that the CISO may approve in writing the use of reasonably equivalent or more secure compensating controls. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that DFS add the word "data" before "classification or sensitivity" to better describe what information a covered entity must track for each asset pursuant to § 500.13(a)(1)(iii). Another commenter suggested that the method to track key information for each asset could apply to "a set of assets."

Response: The Department declines to add the word "data" and to use prescriptive language regarding how covered entities track "classification or sensitivity" or group assets pursuant to § 500.13(a)(1)(iii). Covered

entities must make these decisions based upon their risk assessments. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that DFS add the term "recovery point objectives" to the key information to be tracked for each asset in § 500.13(a)(1).

Response: Covered entities must determine, in accordance with their risk assessment, the information they will track for each asset. The list provided in § 500.13(a)(1) is not exhaustive; covered entities may include additional items or exclude items that are not applicable. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that DFS delete the requirement in § 500.13(a)(1) to track "recovery time objectives" for each asset because tracking this type of information in an asset inventory is unnecessary if tracked elsewhere and may lead to duplication and inconsistencies.

Response: DFS believes that it is important for an asset inventory to include, if applicable, each of the items listed in § 500.13(a)(1), so that a complete asset inventory is available in one place, even if some information is available elsewhere. Therefore, DFS did not make any changes in response to this comment.

Comment: One commenter requested that the Department delete the social engineering training requirement in § 500.14(a)(3) because risks identified in the risk assessment should drive the training.

Response: Social engineering poses a significant and common risk to all entities because it relies on human error rather than vulnerabilities in information systems. Human error has been proven to be a significant risk that has frequently allowed unauthorized access to information systems and nonpublic information. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that DFS remove the word "centralizes" from the requirement for class A companies to implement "a solution that centralizes logging and security event alerting" in § 500.14(b) because it would require a specific solution rather than taking a general principles-based approach.

Response: Centralized logging and security event alerting provide a holistic view of a covered entity's security posture as well as valuable insights into incidents and anomalies. Class A companies, however, maintain the flexibility to determine the most effective solution based on their needs if its CISO approves the use of an equivalent or more secure compensating control. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department reinstate the ability of a covered entity to implement effective alternative compensating controls to encryption of nonpublic information in transit over external networks in § 500.15 because other controls, such as aggregating or de-identifying data, may allow for secure communications. Another commenter requested that the Department add language to § 500.15(a) to provide that "data in use" does not require encryption.

Response: The Department is unaware of any effective alternative compensating control currently being used in the financial services sector that is comparable to encryption in transit over external networks. The encryption requirements in § 500.15 only apply to nonpublic information. If the aggregated or de-identified data does not constitute nonpublic information as defined in § 500.1, the encryption requirements in § 500.15 do not apply. The Department declines to add explicit language regarding the use of encryption for data in use as there may be instances where such data would require the use of encryption, depending on the circumstances and cybersecurity risks to a covered entity. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that the Department include a scope assessment setting out the areas that need to be addressed in incident response plans pursuant to § 500.16(a)(1).

Response: Since any incident response requires a covered entity to conduct a scope assessment, the explicit reference to it in § 500.16(a)(1) is unnecessary. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that the Department make a number of revisions to the requirements regarding business continuity and disaster recovery ("BCDR") plans in § 500.16(a)(2), such as explicitly requiring BCDR plans to be based on a covered entity's risk assessment. Commenters requested specific language changes, such as: (1) replacing the words "at minimum" with "where applicable," so only certain of the enumerated items in § 500.16(a)(2) would apply based on the risk assessment; (2) removing "cybersecurity-related disruption" because it would limit the scope; and (3) adding "supplier failure, service deterioration and concentration risk" as risks that require mitigation strategies.

Response: First, BCDR plans, as part of a covered entity's cybersecurity program, must be based on that covered entity's risk assessment. Second, with respect to the specific language changes requested: (1) the Department believes that it is important that a covered entity's BCDR plan include all of the elements listed in § 500.16(a)(2) and not only those that such covered entity believes to be applicable; however, the emphasis placed on each section will depend upon the entity's risk assessment; (2) the Department declines to remove the words "cybersecurity-related disruption" because this language was added to clarify that the scope of the BCDR requirements are limited to those that are cybersecurity-related; and (3) the Department believes that including "supplier failure, service deterioration and concentration risk" would be unduly prescriptive. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that the Department allow covered entities to maintain on-premises backups pursuant to the requirement in § 500.16(a)(2)(v) instead of offsite backups if the on-premises backups have equivalent cybersecurity controls/protections.

Response: Offsite backups provide an additional level of data security in the event of a physical event, such as a fire or natural disaster. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that DFS: (1) clarify who is considered the highest-ranking executive at a covered entity for purposes of the BCDR and incident response testing requirements in § 500.16(d); (2) clarify

whether the highest-ranking executive is required to physically participate in such testing; and (3) eliminate the requirement for senior officers to participate in these tests.

Response: The Department has replaced the term "senior officers and the highest-ranking executive" with "management" to clarify that the Department's intent is to require different levels of management involvement at different times for different tests as needed to ensure that such tests are appropriately conducted given the risks faced by the covered entity.

Comment: Commenters requested that DFS eliminate the requirement to test the incident response and BCDR plans pursuant to § 500.16(d) or decrease the frequency from every year to every three years or periodically.

Response: The Department believes it is important to test the incident response and BCDR plans at least annually and therefore is not making any changes in light of this comment.

Comment: One commenter requested that DFS clarify whether a BCDR test conducted by the main foreign office of a DFS-licensed branch located in New York would satisfy the BCDR testing requirements in §500.16(d)(1).

Response: A BCDR test conducted by the main branch would be acceptable as long as it satisfies the BCDR testing requirements in § 500.16(d)(1). DFS did not make any changes in response to this comment.

Comment: Commenters asked the Department to align § 500.17(a) with other cyber incident reporting requirements, especially those that will be required under the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").

Response: The Department declines to make changes solely to conform to federal laws since the Department's requirements are tailored to objectives specific to its mission. Nonetheless, the Department is monitoring federal and other incident reporting requirements (CIRCIA's implementing regulations are not expected until 2025) and will continue to adapt its regulation and approach as appropriate and consistent with its

mission. For example, the Department is adding the use of the term "cybersecurity incident" to align with other regulations and industry usage.

Comment: Commenters requested that the Department require covered entities to only report successful cybersecurity events pursuant to § 500.17(a) because, among other things, it would avoid overwhelming the Department with reports that would not be useful to the Department.

Response: The Department has broad authority to safeguard New York's financial services sector, businesses, and consumers and the reporting of unsuccessful cybersecurity events has been useful to the Department in carrying out its broader supervisory responsibilities, such as alerting financial services businesses and related individuals to indicators of compromise and techniques, tactics and procedures of cybercriminals. Therefore, the Department declines to make changes in light of these comments.

Comment: Commenters requested that the Department remove the addition of "at the covered entity, its affiliates, or a third-party service provider", which is used to specify where reportable events may occur in §500.17(a) because the key determination is whether the event impacts the covered entity.

Response: The Department declines to make any changes based on this comment because it is useful to explicitly specify that the notification requirements apply whether the cybersecurity incident occurred at the covered entity, its affiliates, or a third-party service provider.

Comment: Commenters requested that the Department: (1) clarify that covered entities must only notify DFS of a cybersecurity event pursuant to § 500.17(a) when they notify another governmental body, self-regulatory agency, or any other supervisory body as opposed to requiring notification when a party other than a covered entity is required to provide such notifications; (2) remove this notification requirement when third-party service providers suffer a cybersecurity event or, alternatively, exempt instances where third-party service providers are not contractually required to notify the covered entity within 72 hours; and (3) clarify this notification requirement

by adding a materiality or impact analysis component because, for example, requiring covered entities to report non-material events reported to another regulator creates administrative burden with little value.

Response: The Department has revised the language of § 500.17(a) by replacing "from a determination" with "after determining" to clarify that it is the covered entity that is required to notify another governmental body, self-regulatory agency, or any other supervisory body for the notification requirements to apply, and the 72-hour reporting requirement when third-party service providers are involved is triggered when the covered entity makes its determination that reporting is required, making clear that the reporting requirement is tied to the covered entity having knowledge of a reportable event. The Department believes that providing notification to the Department when notice is already provided to another government body, self-regulatory agency, or other supervisory body would not create a substantial administrative burden.

Comment: One commenter requested that the Department eliminate the requirement in § 500.17(a)(1) that covered entities notify the Department within 72 hours of determining that a cybersecurity event has occurred to allow for covered entities to thoroughly investigate and verify the specifics of such event before the 72-hour time period commences to avoid reporting incomplete and incorrect information.

Response: The Department declines to make changes based on this comment because covered entities are not required to notify DFS until they have investigated enough to determine that a reportable cybersecurity event has occurred. Moreover, DFS does not require the reporting of any more information than covered entities have at the time of notification. DFS does not expect investigations to be complete at that time and is aware that information provided may change as investigations proceed. The Department does expect covered entities to provide more complete information later pursuant to § 500.17(a)(2).

Comment: One commenter requested that the Department limit the required notifications to DFS in §500.17(a) to cybersecurity events that impact products and services provided to New York residents.

Response: DFS promulgated Part 500, in large part, to protect unauthorized access to nonpublic information maintained by its regulated entities and the systems that maintain such information. Limiting notifications as requested would restrict DFS's ability to obtain information necessary for DFS to monitor and respond to the threats impacting covered entities. Therefore, the Department declines to make any changes in light of this comment.

Comment: Commenters requested that DFS remove or revise the requirement in § 500.17(a)(iii) that a covered entity notify DFS of "cybersecurity events where an unauthorized user has gained access to a privileged account" because it is overbroad and would lead to overreporting. In particular, commenters requested that DFS: (1) add a threshold of material harm to the covered entity; (2) clarify that the privileged account must be that of the covered entity; and (3) require that the cybersecurity event occur at, or impact, the covered entity.

Response: The Department is clarifying its intent by removing the explicit requirement to notify DFS of all cybersecurity events where an unauthorized user has gained access to a privileged account. Covered entities will continue to be required to notify DFS when any cybersecurity event, including events involving unauthorized access to a privileged account, meets the other notification requirements in the Cybersecurity Regulation.

Comment: Commenters requested that the Department either clarify or remove the requirement in §500.17(a)(1)(iv) to notify DFS of ransomware deployment incidents because it is duplicative of the requirement in § 500.17(a)(1)(ii) to notify DFS of cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity as the deployment of ransomware within a system is never immaterial or would never not create a reasonable likelihood of material harm.

Response: Although unlikely, there may be instances where ransomware deployed within a material part of a covered entity's information systems does not have a reasonable likelihood of materially harming a material part of the normal operations of such covered entity. The Department believes notification to DFS when

ransomware has been deployed is important enough to warrant mentioning explicitly. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that the Department add a materiality, reasonableness, or other qualifier to the continuing obligation to update the Department and supplement the information provided in § 500.17(a)(2) because, as written, the provision is overly broad, could result in over-reporting without corresponding benefits, and it is unclear when a covered entity's duty ends.

Response: In response to these comments, the Department is clarifying the requirement to "update and supplement the information provided" by replacing it with "update the superintendent with material changes or new information previously unavailable" to reflect the Department's original intent. The Department declines to make further changes.

Comment: One commenter suggested that the Department make it easier for individuals and smaller covered entities to certify annual compliance as required in § 500.17(b) by allowing them to check a box if nothing changes from year-to-year.

Response: The Department believes that all covered entities must conduct an annual review of their cybersecurity programs to ensure that they are complying with the applicable requirements of Part 500 even if their cybersecurity programs have not changed since the previous year. The cyber landscape and cybersecurity threats are constantly changing; consequently, it is not possible for nothing to change from year-to-year. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that DFS clarify that the materiality qualifier for certifying compliance in § 500.17(b)(1)(i)(a) applies to both the severity and time of gaps in compliance so that covered entities are aware that they may certify compliance even if they have violated Part 500 pursuant to § 500.20(b) if such violations are temporary lapses that are not material and have been remedied by the time of certification.

Response: Whether a covered entity has materially complied with the requirements of Part 500 applicable to them depends upon many factors, including both the severity of compliance failures and the length of time of those failures. A covered entity that has violated Part 500 pursuant to § 500.20(b) may still be able to certify compliance if the covered entity determines, based upon relevant factors such as the nature and length of the violation, that it materially complied with the requirements set forth in Part 500 during the prior calendar year. Notably, several immaterial violations, when considered in the aggregate, might constitute a material violation, and covered entities must maintain all relevant records, schedules and other documentation and data supporting their determinations and why they were made in accordance with § 500.17(b)(3). Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested the Department clarify that the certification and acknowledgment requirements in § 500.17(b)(1)(i) apply only to new requirements in the amendment after they take effect.

Response: The Department does not believe this clarification is necessary and did not make changes in light of this comment since the Department believes it is clear that covered entities only need to certify their compliance with provisions of Part 500 that apply to them and are effective during the specific certification period.

Comment: One commenter requested that the Department modify the requirement in § 500.17(b)(1)(i)(b) by adding the word "material" before compliance to align with the modification made by the Department regarding the annual certification of compliance, which the Department changed from requiring full compliance to requiring only "material compliance" during the prior calendar year.

Response: In response to this comment, the Department agrees to add the word "material" before the word "compliance" in § 500.17(b)(1)(i)(b) to be consistent with the Department's intent to allow covered entities to certify their compliance with Part 500 if they have materially complied with Part 500 during the prior calendar year.

Comment: With respect to the requirement to submit acknowledgments of noncompliance in § 500.17(b)(1)(ii)(a), commenters recommended that the Department replace the term "fully" with "materially" so that it conforms with the materiality qualifiers added in other sections of § 500.17(b). Otherwise, the language would require a covered entity to file an acknowledgment of noncompliance any time the entity identifies material noncompliance over any 24-hour period.

Response: In response to these comments, the Department is revising the language of § 500.17(b)(1)(ii)(a) to state: "acknowledges that, for the prior calendar year, the covered entity did not materially comply with all the requirements of this Part[.]"

Comment: One commenter requested that the Department clarify that the requirement to identify noncompliant sections of Part 500 when submitting an acknowledgment of noncompliance pursuant to §500.17(b)(1)(ii)(b) does not apply to identifying actions of third-party service providers.

Response: The requirements in Part 500 apply with respect to actions within the covered entity's control, including with respect to third-party service providers that covered entities hire and with whom they conduct business. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters requested that the Department remove the requirement that the highest-ranking executive sign the requisite certifications and acknowledgments that must be submitted pursuant to § 500.17(b)(1) and require CISOs, or other members of senior management to whom a CISO reports, to sign those annual submissions because CISOs are better able to understand whether a covered entity is compliant.

Response: It is important to require that both the CISO, who is the person in charge of overseeing the cybersecurity program at the covered entity, and the CEO or other highest-ranking executive, who is the person in charge of the business, have active involvement with cybersecurity compliance and sign off on the certifications and acknowledgments. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter asked who could sign the annual notices of compliance when the covered entity is a subsidiary of a larger company.

Response: Each covered entity must have its highest-ranking executive and CISO sign the annual submissions required by § 500.17(b)(1), unless the covered entity does not have a CISO, in which case the filings must be signed by the highest-ranking executive and the senior officer responsible for the covered entity's cybersecurity program. The Department did not make any changes in response to this question.

Comment: One commenter requested that the Department create a new exemption category in § 500.19 for solo insurance agent businesses with relatively small revenues.

Response: The Department declines to make this change currently as more time is needed to understand the potential of creating additional categories of exemptions. The Department encourages covered entities to consider whether they qualify for exemptions pursuant to the amendment as the factors that determine qualification have been expanded so more covered entities will qualify for exemptions.

Comment: Commenters requested that the Department exempt covered entities eligible for a § 500.19(a) limited exemption from the certification requirement in § 500.17(b)(1) because New York is the only state that has this certification requirement, it is burdensome for independent insurance agencies, and certain model laws only require insurance companies to certify.

Response: The Department did not make any changes in light of these comments because requiring submission of an annual notification regarding a covered entity's compliance provides assurance to DFS that covered entities are reviewing their cybersecurity preparedness at least once a year and the incremental amount of work needed to prepare such a certification should be relatively small.

Comment: Commenters requested that the Department clarify whether the limited exemption in §500.19(a)(1) applies only if the covered entity and all of its worldwide affiliates have fewer than 20 employees in total. Other commenters requested that the employee count include only independent contractors who have

access to the covered entity's nonpublic information or exclude other outside groups, such as accounting firms and law firms.

Response: The § 500.19(a)(1) exemption is designed for smaller covered entities that lack the resources of larger organizations. This exemption applies only when the covered entity and all its affiliates have fewer than 20 employees and independent contractors worldwide. The Department does not believe it appropriate to limit this exemption to only individuals with access to nonpublic information. If an affiliate's personnel provide any service to, or performs any task for, the covered entity, those individuals must be counted, regardless of location. This includes, but is not limited to, any shared services provided by an affiliate that are used by the covered entity.

With respect to accounting firms and law firms, the specific facts and circumstances must be taken into account. For example, if a covered entity retains the services of a single-person accounting firm and single-person law firm to act as its chief financial officer and general counsel, respectively, and those individuals only perform services for such covered entity and are otherwise involved in the covered entity's day-to-day operations, then those individuals must be counted for purposes of the limited exemption here. The Department is considering providing additional guidance with respect to this limited exemption.

Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested that the Department raise the gross annual revenue limited exemption threshold in § 500.19(a)(2), in light of inflationary and cost pressures on covered entities and to be more in line with the increased employment and total asset limited exemption thresholds in § 500.19(a)(1) and (a)(3).

Response: The Department, after consideration of these comments, agrees that a proportionate increase in the gross annual revenue threshold is appropriate due to the increase in the total asset limited exemption threshold and therefore has revised § 500.19(a)(2) to increase the gross annual revenue threshold to $7,500,000.

Comment: One commenter requested that the Department clarify whether "gross annual revenue" in §500.19(a)(2) includes gross annual revenues from the covered entity and affiliates "located" in New York State and not from worldwide affiliates stemming from business in New York State.

Response: The Department is clarifying this provision to explicitly provide that the gross annual revenue in each of the last three years includes gross annual revenues from "all business operations of the covered entity and the business operations in this State of the covered entity's affiliates." To qualify for this limited exemption, the covered entity must have less than $7,500,000 in gross annual revenue in each of the last three fiscal years from its business operations wherever located and the New York State business operations of its affiliates. The location of the affiliate is not relevant.

Comment: One commenter requested that the Department clarify whether, when calculating the year-end total assets to determine qualification for the limited exemption in § 500.19(a)(3), a covered entity should include only assets of the covered entity and affiliates located in New York State.

Response: For purposes of the § 500.19(a)(3) limited exemption, covered entities must include their total assets, calculated in accordance with generally accepted accounting principles, as well as assets of all affiliates. Limiting the calculation to only assets in New York State or affiliates located in New York State is insufficient. This limited exemption is designed for smaller covered entities that lack the resources of a larger organization. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department clarify whether, for purposes of the § 500.19(b) exemption, "wholly owned subsidiary" has the same meaning as "affiliate."

Response: "Wholly owned subsidiary" does not have the same meaning as "affiliate," which is defined in § 500.1(a). Not all affiliates are wholly owned subsidiaries, and the Department only intends to add this narrower term to the exemption in § 500.19(b). Since "wholly owned subsidiary" is a commonly understood term, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department clarify how much time a covered entity has to come into compliance with Part 500 when it ceases to qualify for an exemption.

Response: Pursuant to § 500.19(h), a covered entity has 180 days from the date that it ceases to qualify for an exemption to comply with all applicable requirements of Part 500. The Department did not make any changes in response to this question.

Comment: Commenters requested the Department add a materiality threshold to the determination of whether the failure to secure or prevent unauthorized access to an individual's or an entity's nonpublic information due to noncompliance with any section of this Part constitutes a violation in § 500.20(b)(1) to, among other things, prevent the Department from "being overwhelmed by filings of immaterial, temporary lapses in compliance that have already been remediated."

Response: The Department does not require covered entities to file notices for temporary lapses in compliance. Furthermore, a covered entity that has failed to secure or prevent unauthorized access to nonpublic information because it is not in compliance with Part 500 is in violation of Part 500; if the impact of the violation is immaterial, that would pertain to damage calculation and how a potential enforcement action might be viewed by the Department. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department extend the 24-hour time frame in the violation provision in § 500.20(b)(2), especially where a cybersecurity event has occurred and third parties are involved, because of the difficulties in detecting cybersecurity events at third-party service providers within a 24-hour period.

Response: The Department declines to make this change since § 500.20(b) is not intended to create a new standalone compliance requirement; it is intended to provide transparency as to the Department's approach to enforcement of non-compliance.

Comment: One commenter requested the Department clarify that the 24-hour period referred to when defining a violation of Part 500 in § 500.20(b)(2) begins when the covered entity knew of a material failure.

Response: The failure to comply with requirements in Part 500 does not depend on when a covered entity becomes aware of such failure. Therefore, the Department declined to make any changes in light of this comment.

Comment: Commenters requested that the Department provide longer transitional periods in § 500.22 for various requirements.

Response: The Department declines to modify the transitional periods because the Department believes the transitional periods are appropriate and covered entities have had advance notice of the transitional periods as a result of the comment periods.