Assessment of Public Comments on the Proposed Second Amendment to 23 NYCRR 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, law firms, and academics regarding the Second Amendment to 23 NYCRR Part 500.

Commenters stated their support for provisions in the amendment, including the: (1) definitions of "covered entity," "independent audit," and "risk assessment;" (2) changes to the cybersecurity program requirements in § 500.2; (3) changes to the vulnerability management requirements in § 500.5; (4) changes to the access privileges and management requirements in § 500.7; (5) changes to the risk assessment requirements in § 500.9; (6) changes to the cybersecurity personnel and intelligence requirements in § 500.10; (7) monitoring and training and logging requirements in § 500.14; (8) requirement to establish a written incident response plan in § 500.16(a); (9) changes in § 500.17(b) regarding the written acknowledgements of non-compliance and the signatories required for the annual notices of compliance; (10) increase in threshold of employee count and assets to qualify for the limited exemption in § 500.19(a); (11) new exemptions for individual insurance brokers, insurance agents, and other licensees in §§ 500.19(e) and (g); (12) changes to the enforcement provision in § 500.20; (13) the effective date in § 500.21; (14) transitional periods in § 500.22; (15) changes in § 500.24 with respect to exemptions from electronic filing and submission; and (16) risk-based approach that is expressly referenced in several parts of the existing regulation, such as with respect to cybersecurity programs.

Comment: Several commenters claimed that compliance with Part 500 should remain more reliant on an organization's risk assessment instead of on prescriptive standards and controls. Other commenters noted that the amendment will cause undue administrative and financial burdens on DFS-regulated entities. Some commenters also are concerned about how they will be able to comply with the new requirements given the currently limited state of the cybersecurity workforce.

Response: Part 500 takes a general risk-based, principles-based approach that the amendment does not change. Part 500 is risk-based and does not mandate unreasonable technical controls. The cybersecurity standards that companies must implement are minimum cybersecurity best practices that the Department believes should be implemented by all covered entities regardless of their risk assessment. However, the manner in which covered entities comply with the provisions is based on their risk assessment. The changes to the definition of risk assessment serve to clarify the existing regulation. The Department has provided adequate transition periods to provide covered entities sufficient time to obtain adequate resources to satisfy the new requirements in the amendment.

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

Comment: Commenters also stated that certain requirements, such as requiring small businesses to eliminate password sharing, are too costly for small businesses, and that templates should be provided for guidance.

Response: The Department has concluded that no change is necessary because the practice of user access through password sharing is unreasonable and all covered entities must exercise minimum cybersecurity practices. Policy templates and other free resources are available on the Department's website through links on the Cybersecurity Resource Center to the Global Cyber Alliance's ("GCA") Cybersecurity Toolkit for Small Businesses. Therefore, the Department did not make any changes in light of these comments.

Comment: Several commenters advocated for additional requirements in the amendment, such as "resilience by design" and the adoption of cloud, software, and technology escrow solutions as a baseline implementation, and the use of threat hunting, machine-learning-based prevention, zero trust, and managed service providers.

Response: Escrow solutions may be appropriate for certain companies and could help mitigate risks, such as software providers going out of business and no longer providing a critical program. Similarly, the technologies

referenced by these commenters are appropriate for some covered entities. Mandating the implementation of certain technologies, however, would limit the ability of covered entities to determine what protections are needed based on their risk assessment. The Department generally attempts to avoid mandating the use of specific techniques or technologies. One exception is multi-factor authentication ("MFA"), which evidence suggests is the best way to avoid breaches and is currently inexpensive and easy to implement. Threat hunting may be included as part of penetration testing or auditing requirements, but a covered entity should be able to determine the type of penetration testing and auditing that is required based on their risk assessment. The use of machine-learning-based prevention and zero-trust architecture are also appropriate measures that companies may take to protect their systems. However, the Department declines to mandate these methodologies at this time to avoid becoming overly prescriptive, especially given the many different sizes and types of entities that the Department regulates.

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

Comment: Several commenters questioned what it means to be "qualified" under both the amendment and existing Part 500 language, such as in § 500.4, § 500.5, § 500.8, and § 500.10. Some commenters suggested changing "qualified" to "competent" or "experienced." Other comments suggested defining "qualified" or including guidance on what constitutes qualified personnel and aligning the terminology with other sections of Part 500. One commenter suggested clarifying that companies have the discretion to determine what qualified means in their organizations to ensure they sufficiently assess the qualifications of testing staff. One commenter suggested that the CISO and other cybersecurity personnel be required to hold recognized certifications or accreditations to be considered qualified.

Response: No particular level of education, experience, or certification is prescribed by the amendment. Necessary qualifications will depend upon the size and complexity of an organization's information system and

the volume and sensitivity of the information maintained. Each covered entity will be required to evaluate its own cybersecurity needs.

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

Comment: Commenters requested clarification regarding the term "industry standards" used in § 500.7(b) with respect to the written password policy and § 500.15 with respect to encryption.

Response: Industry standard is a commonly understood term meaning generally accepted requirements followed by the members of an industry. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters suggested that the Department consider replacing the phrase "reasonably equivalent or more secure compensating controls" found in § 500.7(b), § 500.12, and § 500.14(b) with another phrase, such as "effective alternating compensating controls."

Response: Given the important role that blocking commonly used passwords, implementing MFA, and utilizing the tools referenced in § 500.14(b) have in access control, monitoring, and alerting, any alternative measure should provide at least as much protection and be at least reasonably equivalent or more secure. Therefore, it is not necessary to change the language and the Department did not make any changes in light of these comments.

Comment: Several commenters suggested revising certain provisions of Part 500 so that it aligns with other laws and requirements, such as the Federal Trade Commission's Safeguards Rule ("FTC Safeguards Rule") and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), for example, with respect to not mandating the extent or frequency of certain security controls, audit requirements or governance models, and requiring consistency with the National Institute of Standards and Technology ("NIST") Framework. With respect to CIRCIA, for example, suggestions included aligning reportable cybersecurity events under § 500.17 with the definition of "significant cyber incident" under CIRCIA and aligning the notice and explanation of

extortion payments requirements. One commenter suggested that the amendment could have unintended consequences, particularly for the communications sector and critical infrastructure companies, that Part 500 is already comprehensive, and that there are many other cybersecurity regulations that apply to covered entities, and accordingly, the amendment may not align with federal rules and regulations and may lead to a reduction in cybersecurity.

One commenter suggested deleting § 500.17(a) because, according to this commenter, § 500.17(a) exceeds the reporting framework of CIRCIA, and the Regulatory Impact Statement states that the amendment is consistent with CIRCIA. This commenter also mentions the lack of protections similar to those found in 6 U.S.C. § 681e(b).

Response: The other laws and standards referenced in these comments were considered during the drafting of the amendment, and Part 500 already requires that reasonable and risk-based policies and procedures be implemented. Because Part 500 is a risk-based regulation, covered entities can tailor their compliance to the risks facing their organization. The provisions are flexible enough to allow entities to adhere to the requirements of other federal regulations and are already based on federal cybersecurity standards, including NIST. The minimum requirements in Part 500 ensure that covered entities implement certain baseline cybersecurity protections or controls. The federal rules regarding cybersecurity are limited and do not apply to all the types of entities regulated by the Department.

The reporting requirements for provisions, such as the notice and explanation of extortion payments requirement in § 500.17(c), are consistent with the reporting framework established by CIRCIA and the Department believes that the definition of "cybersecurity incident" used in CIRCIA is too narrow because it would not include many of the successful cybersecurity events that occur at covered entities. The Department has endeavored to harmonize and align where appropriate and practical and believes that any differences are necessary to further the purpose of the amendment.

The Regulatory Impact Statement did not state that the entire notification provision in § 500.17(a) was consistent with CIRCIA, only that the ransomware notifications were consistent. Section 500.18 contains disclosure exemption language similar to that contained in § 681e(b) of CIRCIA. Section 500.17(a) requires notifications as promptly as possible but in no event later than 72 hours "from a determination that a cybersecurity event has occurred," allowing for an initial review of the cybersecurity event and forensic information gathering and review. The Department does not believe that the subtle differences between the notification requirements contained in § 500.17(a) and those contained in CIRCIA justify any changes to § 500.17(a).

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

Comment: Several commenters had questions regarding the Department's security practices or stated that the Department should clarify or adopt clear protections surrounding the processing, use, sharing, and storage of security-related information that it receives from regulated entities, explicitly address the confidentiality of documentation and information submitted, disclose and provide assurances as to how it will protect sensitive information provided by covered entities, and clarify how the information will be used, such as with respect to information provided pursuant to § 500.17. One commenter suggested that subparagraphs (iii) and (iv) of § 500.17(a)(1) be deleted because they are too specific and that a database of such details of security deficiencies would be an attractive target for bad actors, especially because the portal used for reporting is accessible from the Internet.

Other commenters requested that covered entities be permitted to make highly sensitive data available to the Department only on an as-requested basis and had questions regarding confidentiality, such as whether submissions of cybersecurity events would be made public, or suggested including language in the amendment that disclosures to the Department will be maintained in strict confidence and not subject to public disclosure.

Response: The Department takes security very seriously and believes that the protections it has put in place are adequate. Pursuant to § 500.18, "[I]nformation provided by a covered entity pursuant to this Part is subject to

exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable State or Federal law." The purpose of Part 500 is to set forth requirements for covered entities, not for the Department, as the Department does not regulate itself. It also would not be appropriate for the Department to publicly disclose its security practices. Therefore, the Department did not make any changes in light of these comments.

Comment: Several commenters requested that safe harbor provisions be added with respect to various provisions of the amendment, such as with respect to the access privileges and management requirements in § 500.7 if information systems are configured as per a manufacturer or third party configuration standard, or with respect to asset management requirements in § 500.13(a) if a standard methodology is utilized, such as NIST Special Publication 1800-5, IT Asset Management.

Commenters also requested safe harbors with respect to the certification and notification requirements in § 500.17, such as with respect to the annual certification of compliance requirement in § 500.17(b)(1)(i) for unknown or undiscovered violations at the time of certification. Commenters stated that submitting an acknowledgement of noncompliance pursuant to § 500.17(b)(1)(ii) should provide a safe harbor and prevent enforcement actions against the covered entity if remediation is ongoing or completed within the covered entity's implementation timeline and providing a notice and explanation of an extortion payment pursuant to § 500.17(c) should prevent covered entities from being held liable, penalized, or publicly shamed, and otherwise preclude independent investigations of the covered entity absent other potential violations of Part 500.

Response: The Department declines to add safe harbor provisions to the amendment because the Department does not believe this is necessary. The Department does not have any control over manufacturer or third party configuration standards, or standard methodologies, which may change over time or become obsolete as cybersecurity best practices continue to evolve. NIST Special Publication 1800-5, IT Asset Management, itself states that it does not endorse a particular product or guarantee compliance with any regulatory initiatives, and

further states that the responsibility belongs to an organization's information security experts, who should identify the products that will best integrate with its existing tools and information system infrastructure. These configuration standards and methodologies should be used as a guide or as a starting point and further tailored to the specific needs of the organization, to the extent necessary.

Noncompliance disclosed on acknowledgements submitted pursuant to § 500.17(b)(1)(ii) could describe very serious flaws in the covered entity's cybersecurity program that put the covered entity and others at risk. Providing a safe harbor is particularly problematic for this provision because it could have the unintended consequence of encouraging many covered entities to file an acknowledgement of noncompliance out of an abundance of caution and to avoid enforcement actions or violations found in examinations.

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

Comment: Commenters suggested that the Department provide guidance about which cybersecurity frameworks, risk assessment guidelines and standards are acceptable to use, such as with respect to the cybersecurity program requirements in § 500.2 and the risk assessment requirements in § 500.9.

Response: Part 500 does not specify any particular framework, guidelines or standards to follow. Covered entities are free to adopt whichever framework, guidelines or standards would best fit their needs, provided these comply with the requirements of Part 500, including § 500.2 and § 500.9. There are several cybersecurity frameworks, guidelines and standards from which covered entities may choose, including the cybersecurity framework from NIST.

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

Comment: Several commenters requested that the Department do more to support entities, such as by holding meetings for regular stakeholder engagement on cybersecurity matters and working with industry and the administration to promote a collaborative approach to cybersecurity when they report cybersecurity events, and

suggested as an example anonymizing and sharing incident information to improve and support defensive measures taken by private organizations.

Response: The Department is exploring several initiatives to better support covered entities, including the options suggested by these commenters. The Department did not make any changes in light of these comments because these initiatives would not affect the changes proposed in the amendment.

Comment: One commenter suggested that the size and scope of service of continuing care retirement communities ("CCRCs") make them a lower profile target for a cyber-attack and the need for additional cybersecurity requirements is reduced because of compliance requirements under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Another commenter requested that the Department consider the unique attributes of title insurance agents, such as company size and complexity, when determining the requirements that will apply to them because title insurance agents are small businesses and may not be able to comply and remain competitive.

Response: The regulation is risk based, meaning that CCRCs and title insurance agents that have a lower profile target for a cyberattack have a reduced regulatory burden. Part 500 already provides an exemption for small businesses under § 500.19(a) and for entities relying on the cybersecurity program of another covered entity under § 500.19(b). These exemptions will reduce the regulatory burden placed on smaller covered entities.

In addition, Part 500 provides separate cybersecurity requirements, apart from and in addition to those required by HIPAA, that the Department believes are important.

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

Comment: Commenters suggested narrowing the scope of Part 500 to explicitly exclude information systems that do not process or hold information related to financial products or limit the scope of Part 500 to the portion of the business related to an activity regulated by the Department. Another commenter expressed concern

that the Department is creating requirements that are unique to New York for an issue that extends beyond the borders of New York State.

Response: Part 500 applies to entities regulated by the Department. If these entities have multiple businesses, they still need to secure their systems. Requiring entities only to secure the information systems used to house or process financial information would not provide adequate cybersecurity. If the systems are not adequately isolated from the rest of the covered entity's network, a breach of an information system not directly related to banking, financial, or insurance services may lead to a compromise of relevant nonpublic information.

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

Comment: One commenter suggested adding non-human identities to the definition of "authorized user" in § 500.1.

Response: The Department did not make any changes in response to this comment because this definition was unchanged in the amendment and because the Department does not think it is necessary.

Comment: With respect to the "Class A companies" definition in § 500.1, several commenters stated that the definition was ambiguous, including with respect to the revenue thresholds, what being "in this State" means, and which affiliates to include for purposes of determining whether the thresholds are met in this definition. One commenter was concerned that including affiliates outside New York State or not regulated by the Department will cause small companies to fall within this definition and subject them to significant compliance costs.

Several commenters suggested using different metrics, such as an asset-based threshold, a risk-based threshold, or an economic threshold including throughput or volume of client records, or increasing the dollar thresholds.

Other commenters suggested excluding entities operating a separate network or requiring common processes, or common operational and technical infrastructure.

Commenters also stated that the inclusion of affiliates in this definition would capture additional entities, including smaller organizations, such as continuing care retirement communities, and subject these additional entities to the requirement in § 500.2(c) for Class A companies to conduct an independent audit of their cybersecurity programs at least annually, which these commenters stated is burdensome, complex and impracticable.

Response: In response to these comments, the Department is revising this definition by adding language to clarify that when calculating the number of employees and gross annual revenue, affiliates include only those that share information systems, cybersecurity resources, or all or any part of a cybersecurity program with the covered entity. The Department declines to use additional or other metrics in this definition or modify the dollar thresholds because the existing proposed metrics are more easily measured across all covered entities and the proposed dollar thresholds are appropriate. The revenue threshold in this definition specifies that it includes gross annual revenue for the covered entity and its affiliates in New York State.

Comment: With respect to the "Class A companies" definition in § 500.1, one commenter stated that the nexus to New York is overly broad and de minimus in relation to total revenue or employment and would expand covered entities to include those already regulated by other government agencies. Another commenter stated that this definition would cause affiliates of a Class A company to qualify as Class A companies if located in New York State, regardless of whether those affiliates meet the revenue threshold, and requested that the language be clarified to explicitly state that affiliates that do not meet the threshold or are not covered entities do not qualify as Class A companies.

Response: The Department believes that the $20 million in gross annual revenue threshold in each of the last two fiscal years from business operations of the covered entity and its affiliates in New York State is neither overly broad or de minimus, and the appropriate nexus to New York State. Moreover, the definition of Class A companies does not expand covered entities to include those already regulated by other government agencies or

affiliates of Class A companies because the predicate for being a Class A company is that such an entity must be a "covered entity." Whether a covered entity is considered to be Class A depends on its gross annual revenue and number of employees as well as the gross annual revenue and number of employees of its affiliates, but the affiliates cannot become Class A companies themselves unless they are also covered entities as defined in this Part. Therefore, the Department did not make any changes in light of these comments.

Comment: With respect to the "Class A companies" definition in § 500.1, one commenter recommended deleting this definition altogether and making the Class A requirements based on the risk level of data maintained by the covered entity. Another commenter stated that the new requirements for Class A companies are based on inaccurate presumptions of increased risk for Class A companies and may be counterproductive.

Response: The new category of Class A companies is intended to capture certain larger entities and it is not by itself indicative of these entities' risk exposure. Larger entities by their nature have more systems and those systems are typically more complicated, and these larger entities would benefit from the additional controls and tools required for Class A companies. Larger entities may also have a greater amount of non-public information and a breach at a Class A company could have a greater impact. Additionally, larger entities are in a better position and have increased staffing and budgets to implement the cybersecurity best practices required by the amendment as compared to smaller covered entities.

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

Comment: One commenter was concerned about increased administrative costs resulting from, according to this commenter, the requirement for each entity within a group of affiliated entities to fully comply with the regulation individually. One commenter requested that the Department limit the scope of Part 500 to "data and information systems that support regulated activities in which DFS has explicit regulatory authority." The commenter also stated that the inclusion of "Class A companies" would expand the Department's authority and

suggested instead that the Department create a targeted list of covered entities that, if impacted, could create significant consequences.

Response: The comment regarding limiting the scope of Part 500 to "data and information systems that support regulated activities in which DFS has explicit regulatory authority" was unclear to the Department. Covered entities must comply with the portions of Part 500 applicable to them, and Part 500 applies only to those affiliates that are themselves covered entities. Additionally, pursuant to § 500.2, a covered entity may meet the requirements of Part 500 by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of Part 500, as applicable to the covered entity. The addition of the "Class A companies" definition and the new provisions in the amendment that apply to these Class A companies do not expand the scope of covered entities or the Department's authority and creating a targeted list is impractical and would not serve the intended purpose of the "Class A companies" category.

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

Comment: Several commenters proposed that the Department remove the word "unsuccessful" from the definition of "cybersecurity event" in § 500.1 and suggested that notifications pursuant to § 500.17(a) be provided only for successful cybersecurity events. Some of these commenters requested that notifications pursuant to § 500.17(a) be further limited to where material information was accessed, and stated that it otherwise would be overly burdensome to comply and the Department would be overwhelmed by notifications.

Response: The Department concluded that no change was necessary. Removing unsuccessful attempts from the notice requirement would prevent the Department from obtaining information on unsuccessful breach attempts. Furthermore, retaining the current definition of "cybersecurity event" is important for purposes of the reporting requirements of covered entities for instances where notice is required throughout § 500.17(a).

Comment: One commenter suggested that the Department broaden the definition of cybersecurity event to include "data loss and corruption", whether malicious or inadvertent. The commenter claims that this change will make the definition consistent with the definition of cybersecurity program and the incident response provisions.

Response: The Department concluded that no change is necessary. The current definition already covers any deliberate attempt to gain unauthorized access to disrupt or misuse a covered entity's information system, which includes attempts to maliciously corrupt or delete data, and it is not necessary for the Department to be notified every time an entity accidentally corrupts some of its data while managing its own systems.

Comment: With respect to the definition of "independent audit," several commenters were concerned with the external auditor requirement and suggested that the Department allow for internal auditors or permit covered entities to determine, in their discretion, whether an internal audit is sufficiently independent and whether an audit should be done internally or externally. Commenters stated that this would be burdensome, including financially, especially for small- and medium-sized financial services entities, would take staff away from critical operations, and could result in independent auditor scarcity and a backlog making it difficult to meet compliance deadlines. Commenters suggested that internal auditors also be permitted, because internal audit functions can be performed in accordance with professional standards addressing independence, internal auditors have expertise and insight, banking regulators already require banks to maintain independent internal audit programs, and requiring an external audit is not guaranteed to provide additional value. Commenters also discussed the significance of an internal audit function, including independence, and outsourced audit services.

Other commenters suggested revisions, such as precluding an auditor from auditing cybersecurity controls that they were involved in designing or where they have a financial interest in the company being audited, requiring that internal audit personnel not have their compensation determined by personnel that report to the business being audited, and that the internal audit comply with recognized auditing standards and be done annually. Commenters also requested clarification regarding the meaning of audit, the meaning of independence,

such as whether auditors associated with an affiliate of a covered entity could conduct an audit, and regarding the role of internal auditors in engaging with and overseeing external auditors and reporting about external audits to the senior governing body or relevant audit committee.

Other comments were made with regard to timeliness, the possibility of inappropriate marketing by self-interested third party vendors and concerns relating to these vendors having sensitive company information, the lack of CISO direction, and whether a company should have the flexibility to use an external auditor in its discretion, based on its risk assessment or if the Department so determines. Commenters also suggested that the Department set out rules regarding focus, audit methodology, functions, processes, procedures, controls, and reporting structure, and clarify audit scope, criteria and type, expected qualifications and expertise of auditors.

Response: The Department agrees that it would be appropriate to include internal auditors in the definition of "independent audit" and is revising this definition to include both internal and external auditors. This definition requires that auditors be free to make decisions not influenced by the covered entity being audited or by its owners, managers or employees. The Department declines to add additional parameters around an independent audit because the suggestions proposed may not be appropriate for all covered entities, and each Class A company must determine, in accordance with its own auditing and independence standards, how best to structure its audit program.

Comment: One commenter requested that the Department update the definition of "information system" in § 500.1 to include cloud native systems, such as software as a service ("SaaS"). Another commenter stated that the Department should expressly permit companies to determine which devices fall within the scope of this definition because large enterprises will have information systems that process or store nonpublic information that is unrelated to the Department's interests, and many companies use multiple outside or cloud vendors and services and are better positioned than the Department to assess which information systems support Department-regulated or licensed activities.

Response: The Department did not make any changes in light of these comments because the definition of "information system" already covers cloud native systems, § 500.2(b) requires that the "cybersecurity program shall be based on the covered entity's risk assessment," and all devices that pose a cybersecurity risk to the covered entity should be included in the covered entity's cybersecurity program.

Comment: With respect to the proposed changes to the definition of "multi-factor authentication" in § 500.1, one commenter stated that it was pleased that text messaging was removed as an allowable possession factor, and several commenters requested clarification as to whether text messaging is still an acceptable form of MFA. They also noted that some states, including New York, have heightened regulatory scrutiny regarding the use of biometrics and the FTC has begun the rulemaking process for its own restrictions on the collection and use of biometrics. One commenter questioned whether there is an impact to the use of tools like Microsoft Authenticator and stated that it may be onerous for some covered entities to require physical tokens.

Response: This definition was amended to eliminate the reference to text message on a mobile phone. Text message MFA, while still acceptable, is widely considered to be a weaker form of MFA, and the Department encourages the adoption of more secure forms of MFA, in particular phishing-resistant forms of MFA.

The comments regarding biometric laws and regulations are not directly relevant because the amendment does not prohibit text message MFA or mandate that only biometric MFA be used.

Mobile phone authenticator applications, such as Microsoft Authenticator, would satisfy the "possession factor" in clause (2) of this definition, and covered entities are not required to purchase physical tokens. Many possession factors, such as mobile phone authenticator applications, are free.

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

Comment: With respect to the definition of "penetration testing" in § 500.1, commenters requested that certain terms such as "outside" and "service account" be defined or clarified, that the definition be modified so that the covered entities can determine which information systems should be tested based on their risk, and that

further revisions be made to this definition. For example, one suggestion was to require attempting penetration of accounts that have unrestricted access to all data stored on an information system, such as those that connect to cloud environments, and accounts where users are able to change privileges or access controls.

Response: The phrase "from outside or inside the covered entity's information systems" makes clear that a covered entity must conduct penetration testing for both internal and externally facing information systems. In addition, this definition begins with the phrase "any authorized user account or service account", which is intended to cover both human and automated accounts. The term "service account" is a commonly understood term in the information technology industry.

The definition of "penetration testing" includes all information systems, including those located within cloud environments. The Department declines to modify the definition of "penetration testing" to be risk-based.

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

Comment: Several commenters requested that the definition of "privileged account" in § 500.1 be narrowed because including "business operations" would cover too many types of accounts, such as accounts for financial specialists, customer service representatives, human resources, and financial reporting system accounts or claims or policy administration system accounts.

Response: The Department agrees with the comments that including business operations would broaden the scope of this definition beyond its intended purposes. Therefore, the Department made changes accordingly by deleting proposed paragraph (2) of this definition.

Comment: Some commenters expressed concern about the definition of "risk assessment" in § 500.1, stating that certain terms, such as "image and reputation," "other organizations," "other relations," "counterparties," and "critical infrastructure" are unclear, difficult to assess, or overly broad. Other commenters stated that the entire definition was unclear and should be revised to, for example, provide guidance regarding how covered entities should evaluate "service providers" and "vendors" as part of their risk assessment. One commenter suggested that

the definition of "critical infrastructure" only should apply to that which is "owned, operated or controlled by the covered entity." Another commenter requested clarification regarding "vulnerability analysis" and the type of vulnerability that must be identified.

Response: In response to these comments and to further align with the definition of "risk assessment" used in the various special publications from NIST, the Department is revising this definition to remove the portion of this definition that states "[r]isk assessments shall take into account the specific circumstances of the covered entity, including but not limited to its size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors, other relations and their locations, as well as the geographies and locations of its operations and business relations."

The inclusion of "image and reputation" in the definition requires covered entities to consider the harm to their brand that data breaches may have. The inclusion of "critical infrastructure" is necessary because the Department wants covered entities to consider the extent to which a breach at their organization may affect critical infrastructure when conducting their risk assessment. Similarly, the Department believes that the other factors referenced are important to include and for covered entities to consider as part of their risk assessment process. The term "vulnerability" is a commonly understood term in the cybersecurity industry and generally includes a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Therefore, the Department did not make any changes in response to these comments.

Comment: With respect to the definition of "risk-based authentication" in § 500.1, one commenter asked if the use of challenge questions as part of risk-based authentication is still acceptable.

Response: This definition was amended to remove the reference to challenge questions as an example and was not a substantive change. Although the use of challenge questions is still acceptable, the Department encourages covered entities to follow best practices and consider more effective alternatives to challenge

questions when using risk-based authentication. Nonetheless, the Department has decided to eliminate this definition altogether because the term no longer appears in the regulation.

Comment: One commenter stated that for insurance companies within a holding company system, obligations are addressed at the holding company or parent level and requested that the definition of "senior governing body" in § 500.1 be modified to include the ultimate controlling person in a holding company system.

Response: In response to this comment, the Department is adding the following language to this definition: "For any cybersecurity program or part of a cybersecurity program adopted from an affiliate under section 500.2(d), the senior governing body may be that of the affiliate."

Comment: One commenter requested that quasi-governmental entities be excluded from the definition of "third party service providers" ("TPSPs") in § 500.1. Other commenters requested that the Department either exclude all covered entities, or specifically exclude insurance agents and brokers regulated by the Department. These commenters argued that they should be able to rely on the Department's regulation over such covered entities, and that it would be too burdensome for insurance companies to have to conduct diligence on all Department-regulated insurance agents and brokers.

Response: The substantive scope of this definition and the TPSP requirements in Part 500 is unchanged in the amendment.

It is irrelevant whether a third party obtains its funding from governmental sources or enjoys other favorable legal treatment due to its quasi-governmental status. The covered entity must ensure the security of information systems and nonpublic information that are accessible to, or held by, each of its TPSPs.

Additionally, although a TPSP that is a Department-regulated covered entity makes it more likely that the TPSP has implemented the controls mandated by Part 500, a covered entity must make its own determination, based on its risk assessment, regarding the cybersecurity practices a TPSP must have in place for it to do business with the covered entity. The covered entity may require cybersecurity controls and standards beyond what Part

500 requires. Furthermore, a covered entity should not assume that every covered entity is in compliance at all times with Part 500.

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

Comment: Commenters expressed concerns regarding the requirements in § 500.2(c), such as claiming that they overlap with other requirements of the Department. They also requested that the audit frequency be decreased, suggested that the requirement only apply if there were significant changes, like a change in the business or technology causing a material change to the covered entity's cybersecurity risk or information technology strategy, requested that the Department permit companies that comply with other laws or international standards, such as Regulation Systems Compliance and Integrity or the International Organization for Standardization, be exempt from this requirement, or otherwise exempt subsidiaries if audits are conducted at the parent level, and requested that the audit frequency be based on a company's risk assessment.

Response: The Department believes that the independent audit requirement for Class A companies is important and should be performed at least annually. To the extent that a covered entity has adopted the relevant and applicable provisions of a cybersecurity program maintained by a parent entity pursuant to § 500.2(d), the applicable provisions of that cybersecurity program would need to be included as part of the independent audit. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter requested that this provision allow covered entities to redact information that is made available to the Superintendent upon request pursuant to § 500.2(e), stating that "information relevant to the covered entity's cybersecurity program" is too broad and would allow attackers to use those details and increase their chances of success.

Response: The amendment is not changing the requirement in Part 500 to make available to the Superintendent upon request all documentation and "information relevant to the covered entity's cybersecurity program." Covered entities may discuss any concerns about providing specific information during an

examination with the examiner-in-charge and redactions of specific information may be appropriate under certain circumstances, but covered entities should not be able to decide unilaterally the information that they may redact or provide. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested clarification that when adopting portions of an affiliate's cybersecurity program, information inapplicable to a covered entity will not fall under Part 500, and that to the extent these materials are reviewed, this is only for the purpose of reviewing the covered entity's program.

Response: Pursuant to § 500.2(e), documentation and information to be made available to the Superintendent upon request includes "relevant and applicable provisions of a cybersecurity program maintained by an affiliate and adopted by the covered entity." Part 500 only applies to those relevant and applicable portions of an affiliate's cybersecurity program actually adopted by the covered entity. Therefore, the Department did not make any changes in light of this comment.

Comment: Several commenters stated that the Department should require approval of a covered entity's cybersecurity policies in § 500.3 by a senior officer, instead of by a senior governing body. They argue that such approval is not an appropriate function of the board, and that it would require board members to undertake a managerial role given the specificity and technical nature of the required cybersecurity policies.

Commenters also requested clarification with respect to this provision, such as whether the board is expected to participate in direct management of the entity's cybersecurity program and whether the requirement for the senior governing body to approve the cybersecurity policies and procedures only applies for Class A companies.

Another commenter stated that approval of detailed policies should not be permitted to distract the board from its broader functions, an in-depth review of and approval of cybersecurity policies should be reserved for those hired for their cybersecurity expertise who have the capacity to manage those policies, and that to the extent approval is required, the senior governing body should be able to rely on summaries or delegate approval to a senior officer. Another commenter stated that this would require directors lacking the expertise that would enable

them to understand these policies to receive training or explanations from the CISO at every board meeting, taking away from other priorities.

Other commenters requested flexibility and that this provision allow the cybersecurity policy to be approved by either a senior officer or the covered entity's senior governing body, or the board in conjunction with senior management.

Another commenter stated that adding a requirement for annual senior officer approval is too prescriptive if "micro companies" and their risks are considered.

Response: The board of directors or other senior governing body of a covered entity has oversight responsibility over the entity's risks, and cybersecurity risks pervade every area over which the board or other senior governing body exercises oversight. To properly exercise oversight responsibility, the board or other senior governing body must be aware of cybersecurity risks and ensure the company has a written cybersecurity policy and procedures in place. Having the senior governing body approve the policy is the most effective way to achieve this goal, as opposed to relying on an intermediary to directly or indirectly approve and relay that information to the board or other senior governing body.

The requirement that the senior governing body review and approve the cybersecurity policy is important and not too granular or technical. The procedures adopted pursuant to these policies typically would contain much of the specificity and technical aspects that these commenters reference. Procedures, however, do not need to be approved by the board or other senior governing body, and pursuant to § 500.3, need only be developed, documented and implemented in accordance with the written policy or policies.

The arguments that the requirement for the board or other senior governing body to approve policies would be a distraction is not a proper board function, and that the board does not have the requisite expertise to approve these policies is unpersuasive. Pursuant to § 500.4(d), the board or other senior governing body must exercise effective oversight of the covered entity's cybersecurity risk management. In order to do so, the board or other

senior governing body should have sufficient understanding of cybersecurity-related matters, which may include the use of advisors.

This requirement applies to all non-exempt covered entities. All provisions of Part 500 apply to all covered entities that do not otherwise qualify for a full or limited exemption pursuant to § 500.19. The provisions applicable to covered entities that qualify for a limited exemption pursuant to § 500.19(a) are specified in that subsection. The provisions applicable for Class A companies state so in those provisions.

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

Comment: With respect to the requirement in § 500.3 that cybersecurity policies be approved at least annually, several commenters stated that approvals should only be required every two or three years, when material changes are made to the cybersecurity policy, or that this proposed requirement should be removed because of the burden it places on small businesses. Other commenters stated that this section is too prescriptive, the "concept of trigger events" would be more appropriate to determine the frequency, and that obligating board approval for all policies at a large institution is unworkable, especially in view of the frequency and dates of each board meeting.

Response: The Department believes cybersecurity policies must be approved at least annually. If there are no or only insignificant changes since the board last reviewed and approved the policy, and the board has determined that there have been no material changes to risk or operations that would warrant such a change, then they can easily re-approve the policy, but the board first would have needed to consider whether any changes were warranted before doing so. The comment regarding the "trigger events" was not clear to the Department. Regardless, annual (or more frequent to the extent necessary) approval of the cybersecurity policy is not an overly burdensome requirement, especially given the constantly changing cybersecurity threat and cybersecurity landscape.

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

Comment: One commenter states that the language in § 500.3, which provides that policies must be implemented in accordance with documented procedures, is overbroad and will lead to an exponential increase in paper without any appreciable improvement in safety or auditability. This commenter states that it, and other entities, have policies requiring data to be backed-up, which are implemented automatically by the software/hardware systems in use, so a requirement to prepare a written procedure for an automated process would not be appropriate. This commenter suggests that the proposed addition should be revised to require that documented procedures be established for policies that the CISO determines are reasonably necessary to ensure proper implementation.

Another commenter requested that the requirement to develop, document, and implement procedures related to annual written policies be removed due to the burden it would place on small businesses.

Response: The commenter's quoted language is backwards from how it actually appears in the amendment. Section 500.3 requires that "Procedures shall be developed, documented and implemented in accordance with the written policy or policies," and not that policies are to be implemented in accordance with procedures. There is no requirement to document the functionality of software and hardware. Additionally, there are several free template policies and procedures available on the Department's Cybersecurity Resource Center website.

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

Comment: One commenter suggests rephrasing "covered entity's operations" in § 500.3 to "covered entity's cybersecurity-related operations."

Response: The amendment does propose any changes to this language and making the change suggested would result in an illogical conclusion. For example, § 500.3(a) requires the cybersecurity program to address the "information security" of the "covered entity's operations." Requiring the cybersecurity program to include only information security regarding "cybersecurity-related operations" would not cover information security over

any other aspects of the business, which cybersecurity is supposed to protect. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested clarification regarding end-of-life management in § 500.3(c) and the scope of the required policies and procedures the Department expects to be addressed in a company's cybersecurity policies and procedures.

Another commenter stated that a software bill of material ("SBOM") is important and that it should be mentioned in §500.3, noting that a Biden Administration Executive Order requires vendors selling software to the federal government to maintain a SBOM. This commenter requested robust language to include device management for any equipment that touches a network, including mobile device management ("MDM") and prior approval from a designated information security office before connecting any internet of things ("IoT") device to the organization or agency network.

Response: Covered entities must have a cybersecurity policy or policies and procedures that address end-of-life management. The scope of these policies and procedures will vary depending on the covered entity and must be based on the covered entity's risk assessment. The Department does not believe it is appropriate to include additional requirements for SBOM at this point in time because of the current maturity of SBOM for vendors providing software to covered entities, and whether cybersecurity policies and procedures include provisions relating to MDM and IoT would depend on a particular covered entity's risk assessment.

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

Comment: One commenter stated that "although assessments of any number of risks – including privacy, business continuity, data classification, etc. -- are conducted, such assessments are not classified as 'cybersecurity risk assessments.'"

Response: It was unclear to the Department what this commenter was requesting. Section 500.3 requires covered entities to implement and maintain cybersecurity policies and procedures based on its risk assessment,

and address, at a minimum and to the extent applicable to the covered entity's operations, the items listed in §500.3. The items listed in §500.3, including customer data privacy, business continuity and disaster recovery planning and resources, and data governance, classification and retention, are not themselves cybersecurity risk assessments. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter suggested that physical security requirements should be scaled back given the evolving landscape of cybersecurity risk and how low physical concerns fall on the overall risk spectrum. This commenter stated that most companies' information is located in the cloud or co-located in a data center and that the time spent documenting physical security measures, such as video cameras or biometric doors, is no longer a wise expenditure of time or resources, which are considerable. This commenter suggested that a more practical approach would be to only require physical and environmental controls as part of a cybersecurity policy if a company's data is hosted on premises.

Response: Section 500.3 requires covered entities to implement and maintain cybersecurity policies and procedures based on its risk assessment, and address, at a minimum and to the extent applicable to the covered entity's operations, physical security and environmental controls among other controls. A covered entity should determine in its risk assessment which physical security measures are important to the cybersecurity of the company and only address physical security measures, such as video cameras or biometric doors, to the extent applicable to the covered entity's operations. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested the Department provide guidance to less experienced CISOs on how to document issues and report to the Department where the covered entity has decided, against the CISO's authority, not to act, and specify particular nonpublic information thresholds or levels of cybersecurity risk that would warrant reporting.

Response: CISOs and other persons who are concerned about a covered entity's potential non-compliance with Part 500 and other applicable laws and regulations may contact the Department to discuss their concerns. Because this comment did not relate to the amendment, the Department did not make any changes in response.

Comment: One commenter requested that the amendment be clarified such that the CISO is not required to oversee all functions required under Part 500 but may satisfy these requirements in coordination with other senior staff members responsible for functions that meet Part 500 requirements. Specific problematic provisions cited included customer data privacy (§500.3(k)), business continuity and disaster recovery (§500.16) and audit responsibilities (§500.2(c)).

One commenter claims that the amendment would require the CISO to oversee areas it is unfamiliar with.

Another commenter states that the CISO should only be responsible for cybersecurity and can coordinate with other functional areas - specifically data retention and asset inventory.

Response: Pursuant to §500.4, the CISO is responsible for "overseeing and implementing the covered entity's cybersecurity program" and enforcing its cybersecurity policy. Oversight does not mean direct supervision. Proper oversight requires the CISO to be involved, and the CISO cannot simply delegate a portion of that oversight responsibility to another staff member and not be involved. At a minimum, the CISO should be aware of what is being done by other persons with respect to the cybersecurity program and confirm that what is being done complies with the requirements contained in Part 500. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter stated that the reporting chain for the CISO makes a big difference and that organizations need to disclose the reporting chain and relationship with the board of directors and committees. Two commenters requested deleting the provision in §500.4 requiring the CISO to have adequate authority and the ability to direct sufficient resources to implement and maintain a cybersecurity program, stating that this would give the CISO a blank check and the CISO needs to obtain approvals for budget requests.

Two other commenters stated that it was unclear what "resources" were relevant. One of these commenters stated that it was problematic for a CISO at a TPSP to direct sufficient resources and unclear who was responsible for maintaining the cybersecurity program. Another commenter suggested that sufficiency of resources should be replaced with an "appropriately managed" requirement for the CISO to review with the senior governing body the adequacy of the cybersecurity program and disclose any deficiencies in such program, and that the senior governing body would have responsibility to respond.

Two other commenters requested clarification on how to document and demonstrate adequacy and sufficiency.

One commenter suggested replacing "adequate authority" with "autonomy" and replacing "ability to direct sufficient resources" with recommending resources to the senior governing body.

Response: While the reporting chain for the CISO is important, as is the CISO's relationship with the board of directors and committees, the Department believes that it is more important for the CISO to have adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain a cybersecurity program.

The requirement for the CISO to have adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources, does not mean the CISO has a "blank check." The CISO is still subject to a covered entity's regular budgetary approval process. However, an insufficiently resourced cybersecurity program may result in a covered entity's non-compliance with Part 500 if the covered entity is otherwise unable to meet the other requirements contained in Part 500.

Section 500.2 requires the covered entity to maintain a cybersecurity program, and §500.4 requires that covered entity to designate a CISO, a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy, and requires this designated

individual to have adequate authority and the ability to direct sufficient resources to implement and maintain a cybersecurity program.

The new requirements in the amendment are necessary to ensure the CISO is able to carry out the purposes articulated in Part 500. Without adequate authority, the CISO may be placed several levels down in the organizational structure. A junior role would not have the same level of authority within an organization as a senior level executive. Similarly, even a highly experienced and credentialed cybersecurity professional reporting directly to the board of directors or the CEO would be ineffective if not provided with sufficient corporate resource, including personnel or tools, to adequately do their job. Simply "recommending" resources to the board, as one commenter suggested, is insufficient.

However, it is not appropriate for the Department to specify the exact authority or resources every CISO needs. Each covered entity is responsible, in accordance with its risk assessment, for properly maintaining its cybersecurity program, including determining what resources to allocate, and authority to give, their CISO.

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

Comment: One commenter stated that conflict of interest language should be added prohibiting CISOs from being recruited from service providers that provide significant services, because "there is an inherent conflict of interest in the two-hat loyalty created if [the] CISO is not independent."

Response: Designating a CISO that is unable to act in the best interest of the covered entity with respect to cybersecurity would constitute a failure by the covered entity to designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program as required by §500.4(a).

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

Comment: One commenter stated that language should be added requiring the senior governing body to respond to deficiencies reported by the CISO pursuant to §500.4 and acknowledges that §500.5 already requires timely remediation of vulnerabilities.

Response: The requirements in §500.4 for the CISO's report to the senior governing body goes beyond reporting on vulnerabilities, as required by §500.5. If the CISO's report to the senior governing body contained any updates regarding deficiencies that were already fully addressed, there may not be need for the senior governing body to respond. If the report contains unaddressed vulnerabilities and the senior governing body fails to respond, then the covered entity itself has failed to maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information stored on those information systems in violation of §500.2. Additionally, corporate governance laws generally would require a board of directors of a corporation to oversee and address risks in an organization. For example, the duty of loyalty would prohibit a board from consciously ignoring red flags brought to its attention. Therefore, the Department did not make any changes in light of this comment.

Comment: Several commenters stated that it was either overly prescriptive to require annual reporting to the board, inappropriate for the board to receive the update required by §500.4 and that the CISO should report to a senior officer, or that the CISO should be allowed to report to a senior officer, other delegates or the board.

Response: The board of directors or other senior governing body of a covered entity has oversight responsibility over organizational risks, and cybersecurity risks in particular tend to pervade every area over which the board exercises oversight. To properly exercise oversight responsibility, the board or other senior governing body must be aware of cybersecurity risks. Having the CISO report to the board directly is the most effective way to achieve this goal, as opposed to the CISO reporting crucial information to an intermediary and then relying on the intermediary to directly or indirectly relay that information to the board. While delegation may be acceptable for routine reports, a report at least annually to the senior governing body is appropriate. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the annual written report to the board address only "material revisions" to the covered entity's cybersecurity policies and procedures as opposed to a reiteration of unchanged policies and procedure that have been previously in effect.

Response: Section 500.4 requires the CISO to report at least annually on the covered entity's cybersecurity program, and include, to the extent applicable, the covered entity's cybersecurity policies and procedures. In certain circumstances, providing only material updates to the board may be appropriate. For example, it may be appropriate where the board meets frequently and the CISO has been reporting regularly at these meetings and updating the same group of board members informally between board meetings, and the covered entity operates in a stable industry and maintains a mature and up-to-date cybersecurity program. In other cases, such as if several board members are new, or the covered entity operates in a fast-changing, technology heavy industry, such as virtual currency, a full update may be more appropriate.

Regardless, §500.3 requires that the board of directors or other senior governing body approve, at least annually, the covered entity's cybersecurity program. In order for the board of directors or other senior governing body to make an informed decision, it must be properly advised, including pursuant to §500.4 with respect to the CISO reporting, to the extent applicable, on the covered entity's cybersecurity policies and procedures. If the board is already fully aware of certain aspects, §500.4 would not require the CISO to report on those aspects.

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

Comment: Several commenters requested adding a materiality qualifier to the risk assessments update and cybersecurity events examples that are part of the CISO's timely reporting requirement on material cybersecurity issues in §500.4(c).

Response: The items listed in §500.4(c) after the "such as" clause are material cybersecurity issues that the CISO must timely report to the senior governing body. The Department agrees that only significant updates to the risk assessment and significant cybersecurity events must be reported to the senior governing body, to the

extent these are material cybersecurity issues. Insignificant updates to the risk assessment and insignificant cybersecurity events need not be reported.

In response to these comments, the Department is revising the language in §500.4(c) to say "The CISO shall timely report to the senior governing body on material cybersecurity issues, such as significant updates to the covered entity's risk assessment or significant cybersecurity events."

Comment: Several commenters expressed concern regarding the requirement to "timely report" in §500.4, suggesting instead to provide a reasonable set period, define "timely," or replace the "timeliness" requirement with a separate requirement to keep the senior governing body appropriately informed of the covered entity's cybersecurity risk, risk management activities, material cybersecurity issues, and significant updates or changes to the cybersecurity program.

One commenter stated that if "timely" means "at the next board meeting," critical cybersecurity issues are likely to have been fixed by the time the board convenes, which would take away directors' and officers' discretion to devote particular board meetings to other more pressing issues.

Response: Due to the broad scope of what could be considered a material cybersecurity issue that needs to be reported to the board, specifying a time period or otherwise using a different standard such as promptly, or as soon as practical, is difficult. If the covered entity is suffering an ongoing ransomware event, where systems were encrypted and backups are unavailable, immediate notification to the senior governing body is likely warranted. If the information security team is seeing a pattern of increasingly sophisticated intrusion attempts into its information systems, which have thus far failed, an evaluation of the cybersecurity posture and possibly additional resources may be warranted if existing systems are barely keeping up with intrusion attempts, and depending on the seriousness of the situation and how often the senior governing body meets, may require their involvement prior to the next regularly scheduled meeting. Less urgent matters on the other hand could wait until the next time the senior governing body meets as part of their normal schedule.

"Timely" is the best descriptor of how quickly the board should be notified. Therefore, the Department did not make any changes in light of these comments.

Comment: A group of commenters suggested that § 500.4(c) provide for reporting to be live and in person and stated that written reports do not provide the same benefits and increased interactions between the CISO and board improves the CISO's informal authority and improves their ability to manage the firm's security, improving the authority.

Response: Section 500.4(c) requires the CISO to timely report to the senior governing body regarding material cybersecurity issues. The Department declines to prescribe the method of delivery because it should depend on the complexity of the company and the composition of the senior governing body. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested §500.4(d) be deleted entirely because it ignores the CISO's obligation to report to the board in §500.4(b).

Several commenters were concerned that §500.4(d) requires boards of directors to undertake a managerial role. One of these commenters states that companies should not have mandates on how they select and use their boards of directors without flexibility for variation in such companies' approaches that account for their unique risk profiles.

Several commenters suggest deleting the language "and provide direction to management on" in §500.4(d)(1) to clarify that the board provides only oversight, and several commenters state that this language requires board members be directly involved with the day-to-day management of the covered entity's cybersecurity program, a role that is management's job.

One commenter states this subsection presents a significant new risk of corporate director and officer liability, because directors may be liable where they failed to oversee the company's obligation to comply with positive law or positive regulatory mandates, and that the amendment are likely to increase the incidence of

shareholder derivative suits, and that this could increase the cost of directors' and officers' liability insurance and may even disincentivize qualified individuals from serving on corporate boards.

Response: In response to these comments, the Department is deleting "and provide direction to management on" from §500.4(d)(1). The board's primary duty is oversight. Many of the commenters misunderstood the requirement as implying that the board is required to become involved in the day-to-day operations of management. The board must determine the strategic direction of the corporation, and delegate to management the operational duties and directives to pursue that objective.

The argument that this subsection is unnecessary because it is duplicative of §500.4(b) is unpersuasive. This subsection relates to requirements of the senior governing body, while §500.4(b) relates to an obligation of the CISO to provide reports, at least annually, to the senior governing body.

The argument that the amendment would increase the incidence of shareholder derivative suits may ultimately prove to be accurate, but the amendment by itself is unlikely to increase shareholder derivative suit liability on directors, assuming the board of directors complies with the new board requirements.

With respect the argument that the amendment could increase the cost of directors' and officers' liability insurance, no additional details were provided by this commenter on how this possibility "could" occur. Costs could also stay the same or possibly decrease if the company is able to demonstrate a robust cybersecurity program. The amendment will increase the minimum baseline for companies' cybersecurity posture. For there to be a shareholder derivative lawsuit involving a cybersecurity claim, a cybersecurity incident or other cybersecurity-related failure must have first occurred. Raising the minimum baseline will likely decrease the incidence of cybersecurity failures.

Lastly, with respect to the argument that the amendment could disincentivize people from joining the board, the commenter did not articulate why they would be disincentivized. If it is because of increased potential shareholder derivative claim liability, that appears unlikely to the Department. Board members already have a

general oversight obligation, and a potential board member being disincentivized from joining simply because they would have oversight over cybersecurity-related risks, a critical area of enterprise risk, seems unlikely.

Comment: Commenters suggested replacing board of directors in §500.4(d) with senior governing body or otherwise removing or revising the requirements in this provision because the existing regulation already requires covered entities to develop, implement, and maintain a cybersecurity program, and covered entities should not be subject to requirements on how they organize their boards of directors and how those boards conduct risk management with senior leadership, as this would result in the Department inserting itself into how covered entities design their plans to detect, respond to, and recover from cybersecurity incidents.

Response: In response to these comments, the Department is revising §500.4(d) to state: "The senior governing body of the covered entity shall: (1) exercise effective oversight of the covered entity's cybersecurity risk management; (2) have sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors; and (3) require the covered entity's executive management or its designees to develop, implement and maintain the covered entity's cybersecurity program."

Comment: One commenter asked for flexibility in §500.4(d) based on the individual governance structures of insurance groups to allow insurers to maintain the information security program at the group level and to make them applicable to the covered entities.

Response: Covered entities that do not maintain their own cybersecurity program are permitted to meet the requirements of Part 500 by adopting all or a portion of the cybersecurity program maintained by an affiliate, in accordance with the requirements of §500.2(d). Where such cybersecurity program is maintained by an affiliate, the relevant board of directors or equivalent or applicable committee thereof should be that of the affiliate. Therefore, the Department is revising the language in §500.4(d) to say: "The senior governing body of the covered entity shall …" because the definition of senior governing body in §500.1 is flexible and includes affiliates.

Comment: With respect to the requirement in §500.4(d)(3) for the board of directors to have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management, a group of commenters were supportive of this requirement because, according to these commenters, cybersecurity expertise on the board strongly influences the quality of board oversight, and the lack of expertise leads to superficial, check-the-box oversight.

With respect to the requirements in §500.4(d)(3), several commenters recommended defining "sufficient expertise and knowledge," providing guidance on how to prove or demonstrate that the board meets this requirement, or altogether deleting this requirement because for certain entities such as banks, directors receive mandated risk and cybersecurity-related trainings and are provided handbooks. Some commenters suggested using instead the phrase "appropriate understanding of cybersecurity-related matters to facilitate oversight" and stated that boards are deliberative bodies tasked with oversight of many issues, including cybersecurity, and a board with sufficient education and knowledge is able to discharge its various oversight obligations.

Other commenters stated that having cybersecurity experts might not produce the desired outcome, that the Department should not dictate or suggest which experts sit on a company's senior governing bodies, that cybersecurity talent is scarce globally, and it is unclear where companies would obtain this expertise.

Other commenters asked if a CISO or its designee is an appropriate board cybersecurity advisor, or suggested explicitly including that these individuals are qualified to advise the board.

Response: The Department understands the confusion around the phrase "expertise and knowledge" and did not intend to suggest that cybersecurity experts are required on the board. A board should, however, have sufficient understanding of cybersecurity-related matters so they can exercise effective oversight of cybersecurity risks management, which may include the use of advisors, such as the CISO.

Commenters who suggested that this provision was unnecessary because directors already have minimum knowledge requirements via handbooks and training provided by other regulatory bodies, such as the federal

banking agencies, assume that all regulated entities are subject to the same requirements of these other regulatory bodies and that those who received the handbooks and training necessarily would have the requisite knowledge and understanding to fulfill their cybersecurity risk oversight obligations. Being provided handbooks and training alone does not guarantee a sufficient understanding of the subject matter of that material.

According to the National Association of Corporate Directors, "Cyber literacy can be considered similar to financial literacy. Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business." *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards, NACD: Internet Security Alliance* (quoting from another NACD whitepaper, *Cybersecurity: Boardroom Implications*, 2014).

Therefore, the Department is revising §500.4(d) by replacing paragraph (3) with a requirement to have sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors.

Comment: Commenters stated that the FTC Safeguards Rule contains an exemption from penetration testing for companies with fewer than 5,000 customers and one commenter requested that the Department encourage small or limited exempt entities to use continuous monitoring, which, according to this commenter is real-time cybersecurity, as opposed to an annual penetration test and because continuous monitoring "negates the need for an annual risk and vulnerability assessment since this is already an on-going process in continuous monitoring."

Response: Part 500 contains several exemptions listed in §500.19 and the Department does not believe adding a new exemption for covered entities with fewer than 5,000 customers is necessary. Penetration tests reveal vulnerabilities that continuous monitoring does not.

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

Comment: One commenter stated that any requirements related to patching and managing vulnerabilities should be developed in a manner consistent with The Cybersecurity & Infrastructure Security Agency's ("CISA") binding operational directives ("BOD"), such as BOD 20-01, and industry best practices and international standards for vulnerability disclosure programs.

Response: The Department does not believe that adding a requirement to implement and maintain a vulnerability disclosure program is appropriate for covered entities at this time. A vulnerability disclosure program is different from the vulnerability management requirements in §500.5. CISA's BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, requires federal agencies to develop and publish a vulnerability disclosure policy ("VDP") so the public can report vulnerabilities to those agencies. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter stated that technology has made vulnerability management requirements obsolete, and that an annual penetration test by an expert will not provide any greater level of security to an entity that uses existing options that go on continuously. According to this commenter, a non-prescriptive requirement of ongoing or frequent analysis of areas of potential exposure would be more effective.

Response: The benefits offered by penetration testing and continuous monitoring are different. Both are important components of a layered cybersecurity defense. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter stated that §500.5(a) is too prescriptive, and Class A companies should be allowed to conduct internal penetration testing without relying on external independent providers and be allowed to make their own risk-based determination of an appropriate time frame for vulnerability scanning and not default to bi-annual scanning.

Response: This commenter misread the amendment. All non-exempt covered entities, including Class A companies, must, pursuant to §500.5(a)(1), conduct penetration testing by a qualified internal or external party at

least annually. Internal personnel are permitted, and the requirement is at least annually and not bi-annually. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter stated that constant vulnerability management will require additional staff, third party contracts and the purchase of costly scanning and monitoring tools. This commenter recommends keeping the bi-annual vulnerability assessments, with additional monitoring of systems or targeted assessments performed at an interval determined by the covered entity based on its risk assessment.

Response: Penetration testing and system scanning are important for proper vulnerability management. Although there will be additional costs involved for those entities that do not have these programs in place, the risk and potential losses from cybersecurity incidents far outweigh those costs. The Department believes that the "at least annually" frequency is appropriate. Therefore, the Department did not make any changes in light of this comment.

Comment: Several commenters request that penetration testing be based on the risk assessment and that the changes in § 500.5 should not be made, because the new requirements would be costly, burdensome, and disruptive to their operations and existing procedures. Additionally, two commenters request the frequency of scanning be based on the risk assessment. One commenter states the amendment does not specify what systems or networks need to be scanned, and requests that companies be permitted to make risk-based determinations about which systems to scan, at what frequency, and for what vulnerabilities.

One commenter stated that large communications companies conduct testing and scanning that are tailored to their particular systems, and mandated testing at government set intervals could cause instabilities leading to the corruption or loss of data as well as unintentional denial of service. This commenter argues that it is not feasible to test all of a large organization's systems annually while maintaining critical operations because there are not enough highly capable penetration testers and requested clarification that companies be allowed to choose what kind of penetration testing is done.

One commenter stated that if an application is only accessible to internal users from within a covered entity's internal network, and the network itself undergoes penetration testing, it may be unnecessary to separately conduct a penetration test of the application itself.

One commenter stated that § 500.5 is impacted by the requirement in § 500.2 for manual scans and the broad definition of "information system" in § 500.1.

Response: Section 500.5 requires covered entities to, "in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management" that are designed to assess the effectiveness of its cybersecurity program. These policies and procedures shall ensure that covered entities conduct penetration testing "at least annually" and automated scans of information systems, and a manual review of systems not covered by such scans, "at a frequency determined by the risk assessment."

The requirement to maintain policies and procedures to conduct penetration testing and scanning is based off the covered entity's risk assessment. Each covered entity must determine, in accordance with the risk assessment, which systems and portions of its network to include as part of the penetration testing and scanning. For example, decommissioned and disconnected computers need not be scanned, and airgapped systems in a locked room may not be subject to the same type of penetration testing as the rest of the covered entity's information system. Penetration testing for isolated networks may entail, if the covered entity chooses to do so, testing the physical security of the locked room to attempt to gain entry to those airgapped systems. It may not be possible to include airgapped systems as part of an automated scanning software's scope, so those systems must still be reviewed to ensure they are running the latest patches and updates. The frequency of such testing must also be in accordance with the risk assessment but must occur at least annually with respect to penetration testing and is explicitly stated to be "at a frequency determined by the risk assessment" for scanning. Many new vulnerabilities are disclosed each year, and the at least annually frequency for penetration testing will ensure newly disclosed vulnerabilities are included.

The comment that it may be unnecessary to test an application when the network itself undergoes penetration testing assumes that the only purpose of penetration testing is to test against remote attacks, likely from an external source, and ignores insider threats or users who have fallen victim to social engineering and allowed an attacker access to their systems, where once on their system, boundary and network-layer defenses are meaningless.

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

Comment: One commenter requested that "automated scans" be defined or clarified in § 500.5 and asked whether the scan is expected to be internal, external, or both.

Response: The Department believes that the term "automated scans" is clear, and the purpose is stated in § 500.5, namely "for the purpose of discovering, analyzing and reporting vulnerabilities." These scans must be able to reach the covered entity's information systems, and covered entities must determine how best to accomplish that, whether it's internal, external, or both. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter asked what makes a vulnerability "publicly known" and states that not all publicly known vulnerabilities are equally dangerous. This commenter requested confirmation that compliance can be achieved by using a widely accepted, legitimate vulnerability repository, such as the CISA's Known Exploited Vulnerabilities Catalog ("CISA-KEV").

Response: The term "publicly known" is no longer used in § 500.5 and was removed in the amendment. Section 500.5(b) requires that covered entities are promptly informed of new security vulnerabilities by having a monitoring process in place and § 500.5(c) requires that covered entities timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity. The amendment requires vulnerabilities to be prioritized and remediated based on the risk they pose to the covered entity.

There are several vulnerability databases that covered entities may choose to use, including CISA-KEV that this commenter references. Although CISA-KEV is free, companies may choose, based on their risk assessment, whichever resource best fits their budget and needs.

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

Comment: One commenter stated that they do not believe that it is feasible to require a manual review of any systems not covered by automated scans, so this requirement should be deleted.

Response: This commenter did not articulate why they did not believe manual reviews of systems was not feasible. The purpose for both automated scans and manual reviews is stated in § 500.5(a)(2), which requires automated scans and manual reviews "for the purpose of discovering, analyzing and reporting vulnerabilities."

For situations where automated scans do not cover particular systems, those systems must be manually reviewed. For example, if a newly disclosed vulnerability shows that a particular version of an operating system or application is vulnerable to a local exploit and privilege escalation, covered entities may wish to manually verify they are not running those vulnerable software versions and patch or upgrade affected systems, to the extent their automated scans are not capable of reaching such systems.

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

Comment: One commenter stated that entities will need to purchase the technology and training needed to perform automated scans, and manual scans on systems that do not support automated scanning result in a greater workload for technology staff or costs for third party assistance.

Response: To the extent a covered entity is not currently scanning and does not have the staff or resources to manually review systems that, according to their risk assessment would pose a risk to the covered entity, then they would need to invest in additional resources. There may be low cost solutions that would fit their situation, but it is up to the covered entity to determine, based on their risk assessment, what is appropriate based on their

size, complexity and other requirements. Cost alone is an insufficient reason to not undertake this effort. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested clarification on the terms "major system change" and "promptly" used in § 500.5(a) to avoid an excessively broad and costly application of this requirement. According to this commenter, the terms "promptly" and "major" are subjective, and this is a concern because performing a scan after every change is cost prohibitive.

Response: The Department believes that the term "promptly" is clear. In response to this comment, with respect to the term "major", the Department is replacing this term with "material", which is used elsewhere in Part 500 and is a more understood term.

Material system changes are typically planned events. Scans and manual reviews should be planned and coordinated in connection with those events and performed promptly following those changes. To the extent unplanned and done reactively, such as changes made in response to a cybersecurity event or ransomware event, it is even more important to perform a post-change verification automated scan or manual review to ensure no new gaps in cybersecurity defenses have been introduced.

Comment: With respect to the requirement in § 500.5(c) to timely remediate vulnerabilities, one commenter requested that this should apply only to critical and high-risk vulnerabilities.

Response: Section 500.5(c) requires covered entities to timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity. There is no materiality standard in § 500.5(c). All vulnerabilities should be remediated in a "timely" manner. Certain vulnerabilities prioritized as critical by the covered entity may warrant an immediate response. Covered entities may decide to delay for a few days the remediation of certain other vulnerabilities so they can perform internal testing and validation of newly released patches to ensure no additional issues are introduced into their environment. Covered entities may give a lower priority to certain vulnerabilities for remediation due to compensating security controls in place or inherent

difficulty to exploit. Covered entities may also have a monthly or other periodic patching cycle for routine software update releases for non-critical vulnerabilities.

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

Comment: Several commenters requested clarification regarding the terms used in § 500.5(d), including what constituted a material issue, and senior management, and confirmation that the senior governing body is not expected to participate in direct management. Several commenters provided recommendations on what should be reported and the appropriate recipient of those reports, such as un-remediated vulnerabilities and only to the relevant executive or only to senior management. Two commenters suggested adding this to the annual CISO report requirement in § 500.4.

Response: The Department agrees that material cybersecurity issues discovered during testing should be reported to the senior governing body and that this requirement exists in § 500.4(c). Therefore, the Department is deleting the requirement in proposed § 500.5(d).

Comment: One commenter suggested that it would be too burdensome to comply with the two new requirements in § 500.17(a) due to the broad definition of "privileged account" and that it would be particularly challenging for larger covered entities that routinely maintain thousands of user accounts enterprise-wide. Other commenters expressed concern stemming from the inclusion of the term "business operations" in the definition of "privileged account" in § 500.1 and requested clarification whether and when individual access needed to be approved and whether contracted services or responsibilities related to a job's core responsibilities could be permitted.

Response: The Department is narrowing the definition of "privileged account" in § 500.1 by removing language regarding accounts that could be used to affect a material change to the technical or business operations of the covered entity, to the extent they could not otherwise perform security-relevant functions that ordinary users are not authorized to perform.

Comment: Some commenters suggested limiting the applicability of § 500.7 to a covered entity's personnel.

Response: Limiting the requirements to personnel would result in these requirements not applying to independent contractors, consultants, TPSPs, and other parties who are provided accounts with access to a covered entity's information systems and pose the same risks as accounts used by personnel. Therefore, the Department did not make changes in light of these comments.

Comment: Commenters stated that certain requirements contained in § 500.7(a) were unclear, such as with respect to user account access, controls relating to privileged accounts, privileged access criteria, what "promptly" meant for terminating access following departure, and what the term "access" meant. These commenters stated that the requirements may not reflect the intention of the amendment, that cloud environment vulnerabilities are not addressed, and the requirement to promptly terminate access should be subject to a risk assessment of the specific departure. Another commenter suggested specified language changes, such as including the phrase "implement the concept of lease privilege" or adding "and no more" to the end of § 500.7(a)(2).

Response: Cloud environments are covered by the definition of information systems in § 500.1, and the requirements contained in § 500.7 apply to information systems of the covered entity both on-premises and located in the cloud. The section has clear obligations in relation to, among other items, user account access, controls relating to privileged accounts, and privileged access criteria, and the term "access" is a commonly understood term. The requirement to promptly terminate access following departures is clear and no explanation for when a delay in terminating access would be justified by a risk assessment. It was unclear to the Department what additional changes were being requested by these commenters, and some commenters did not request any specific change. The Department declines to make the specific language changes requested because the Department does not believe they are necessary, and the requirements contained in § 500.7(a) were clear and certain smaller covered entities may find it easier to follow the requirements as they are described in this section

as currently drafted without the use of specific cybersecurity terms of art that may be vague. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters stated that the requirements in § 500.7(a) were unclear, lack third party standards, are costly, are prescriptive, and would not result in additional risk mitigation, such as with respect to the requirement to periodically, but at a minimum annually, review all user access privileges, and the requirement to disable or securely configure all protocols that permit remote control of devices, and suggested that these be based on the risk assessment or that the CISO allowed to approve deviation from these requirements. One commenter stated that the requirement for a minimum annual review is inadequate because, for example, it does not take into consideration shifting roles and responsibilities. One commenter believed that §500.7(a)(5) applies to remote desktop protocol vulnerabilities.

Response: Section 500.7(a) states that the requirements set forth therein are required as part of a covered entity's cybersecurity program, "based on the covered entity's risk assessment", which means they already encompass risk-based decision-making, and based on the risk assessment, the CISO has discretion, except for minimum necessary requirements specified in this provision, compliance with which can also be shaped somewhat by the risk assessment. The requirements specified in this provision are clear as to what is required. User access privilege review is a risk mitigation tool that businesses of all sizes should utilize as a basic cyber hygiene measure and the Department has links to many free resources available on its website. The requirement in § 500.7(a)(5) can be satisfied by disabling or securely configuring all protocols that permit remote control of devices, including the remote desktop protocol. Other requirements contained in Part 500, such as § 500.5 with respect to vulnerability management, directly address vulnerabilities discovered in remote desktop protocol applications. Therefore, the Department believes these are basic requirements that should be a part of the cybersecurity program and did not make changes in light of these comments.

Comment: One commenter asserted that the Department should clarify that regulated entities can determine the devices and functions for which limitations of remote control are warranted. For example, by narrowing the application of this requirement to a subset of all network devices, such as mission-critical systems. The commenter also said that the Department should amend § 500.7(a)(5) so it does not appear to require perfect security.

Response: The Department has determined that no change is necessary because allowing remote control of any device on a network, including noncritical ones, to be compromised would put all of a covered entity's devices accessible from the same network at risk, and nowhere does Part 500 require perfect compliance.

Comment: Commenters suggested that § 500.7(b) be revised, for example, to be risk-based, or only have the written password policy requirement apply when accessing an internal network from an external location. Commenters also recommended that the Department provide guidance for certain matters, such as MFA in relation to password use, or controls or risks that need to be managed in connection with privileged access management tools and effective controls. Another commenter suggested that the Department set out steps companies should take when a username and password appear on the dark web, including relating to changing passwords. Commenters also requested clarification around items and terms, such as privileged access management, commonly used passwords, and what types of measures would be considered reasonably equivalent or more secure and suggested that the Department provide vaulting as an example and provide vendors and expectations for a solution.

Response: The written password policy is important to secure access to accounts and is not limited to only when accessing an internal network from an external location. The additional requirements specified in §500.7(b) were implemented for Class A companies because they have the resources to implement controls for privileged access management and automated password blocking and would benefit more from these additional tools because of their more complicated information systems.

Any guidance issued in connection with the requirements contained in Part 500 will not affect the language of the amendment. The Department does not endorse any particular vendors or products. The Department believes that covered entities must themselves determine what vendors and products would best suit their needs, along with the steps to take when a username and password appear on the dark web and the frequency passwords must be changed, each in accordance with the risk assessment. The Department declines to add additional requirements at this time.

There is ample public information on commonly used passwords. The term privileged access management solution refers to a specific type of product and the term is commonly understood in the industry. The Department notes that password vaulting is different from privileged access management. Privileged account management is a domain within identity and access management that focuses on monitoring and controlling the use of privileged accounts, while password vaulting involves storing usernames and passwords for multiple applications securely. In accordance with § 500.7(b)(2), the CISO must approve in writing any instances where blocking commonly used passwords is infeasible and be comfortable with 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 recommended limiting the requirement in § 500.7(b)(2) with respect to an automated method of blocking commonly used passwords to assets that are directly owned and managed by the covered entity as this may not be feasible for third party applications and services, and stated it is unreasonable for CISOs to approve in writing compensating controls for each affected application or service.

Response: In response to this comment, the Department is revising the requirement to apply "on information systems owned or controlled by a Class A company and wherever feasible for all other accounts." Where blocking commonly used passwords is infeasible, reasonably equivalent or more secure compensating controls must be implemented and approved in writing at least annually by the CISO.

Comment: Several commenters stated the application security requirements in § 500.8 and the annual review of such policies and procedures is too burdensome, such as for Class A companies with voluminous procedures and guidelines. Commenters proposed longer timeframes, such as every two years, or that the review be based on a risk assessment, triggers that the entity identifies, or other factors. Another commenter noted it was not clear whether covered entities have to perform a review and update as necessary or at least annually.

Response: The Department did not make any changes in light of these comments. An annual (or to the extent necessary, more frequent) review of written procedures, guidelines and standards by the CISO (or qualified designee) is not an overly burdensome requirement, especially given the constantly changing cybersecurity threat and cybersecurity landscape.

Comment: A commenter noted it is costly to have a small business conduct a risk assessment annually as required in § 500.9(c). This commenter suggested excluding from this requirement covered entities entitled to limited exemptions pursuant to § 500.19(a), except under certain circumstances, such as material breaches or organizational changes, provided the covered entities monitor cybersecurity events and perform vulnerability monitoring. Similarly, another commenter suggested exempting a covered entity from the risk assessment requirement if it has not experienced material changes to its cybersecurity risk.

Response: It is important that covered entities, including small businesses, review their existing risk assessment at least annually to confirm whether all the risks identified therein are still applicable and determine whether any updates are required, even if it ends up imposing an additional cost on the entity. Thus, the Department declined to make changes to § 500.9(c).

Comment: Some commenters requested clarification on the requirement in § 500.9, such as the type and extent of review required as part of the risk assessment.

Response: The type and extent of review required for a risk assessment will vary depending on, among other things, a particular covered entity's business, the type and amount of data it maintains, the cyber landscape

at the time of the assessment, and its cybersecurity risks. Section 500.9(a) requires that the risk assessment be sufficient to inform the design of the particular cybersecurity program and allow for revision of controls to respond to technological developments and evolving threats. Thus, the Department declined to make changes in response to these comments.

Comment: A commenter noted covered entities should be provided with flexibility to decide the frequency of a risk assessment and decide whether an annual review is required as it may be costly. Another commenter noted the timeframe to review and update a risk assessment was overly prescriptive and suggested the Department clarify what constitutes "a material change to the covered entity's cyber risk." Another commenter indicated the phrases "material change" and "cyber risk" were ambiguous and required clarification. Further, another commenter asserted the provision was confusing because a covered entity may not know whether a change is material prior to assessing the risk of the change and recommended modifying the language in § 500.9(c).

Response: The cybersecurity landscape is evolving, and covered entities need to reassess risks, threats and vulnerabilities and update risk assessments, at least annually, or more frequently. Thus, the Department concluded the requirement is not too prescriptive. Part 500 covers a broad range of covered entities that vary in size, type of business and scope of operations. The term "material changes" was not defined as such changes may vary depending on the type of covered entity, size, business, and scope of operations. Therefore, the Department did not make any changes in light of these comments.

Comment: The Department received comments suggesting it delete § 500.9(d) from the proposed regulation. Several commenters opposed requiring Class A companies to use external experts to conduct risk assessments and suggested risk assessments be conducted internally. Commenters generally stated the requirement would be costly, prescriptive, time-consuming, and require personnel at covered entities to spend time working and educating external experts about their organization. It was also noted the requirement is burdensome and moves away from a risk-based approach, especially for small and medium financial service

entities, and the risk assessment and audit requirements for Class A companies rely on an inaccurate presumption that Class A companies have more risk and focus less on the entity's risk profile. Commenters noted this requirement would mainly benefit external auditors and distract covered entity's personnel from their focus on the implementation and maintenance of effective programs and appropriate cybersecurity protections.

Commenters believe covered entities should be able to conduct risk assessments internally as they have CISOs and other personnel that have the requisite expertise, skill and knowledge of the covered entity's business operations, its complexity and structure to conduct them. One commenter noted Class A companies have internal experts since the Department's cybersecurity regulations are the most rigorous in the United States. Another commenter pointed out it is easier for in-house cybersecurity experts to identify weaknesses than external parties.

Commenters expressed concerns that risk assessments performed by external experts may not add value or lower risk. A commenter noted companies with well-defined risks tolerances that have not experienced major changes may not benefit from having an external expert conduct a risk assessment. External parties may not have the same level of knowledge about the covered entity as internal parties, which may impact the accuracy of the risk assessment or result in inefficiencies and delays. Moreover, it was noted that external parties may possibly use the risk assessment for sales purposes, which may result in bias finding. Additionally, a commenter did not believe it was necessary to have an external firm perform a risk assessment to ensure management considers the external environment.

A commenter also stated the requirement for Class A companies to perform an external risk assessment is duplicative of the risk assessment requirement pursuant to § 500.9(c). The commenter indicated that Class A covered entities should have the option to use an external party for either the independent audit or risk assessment. Another commenter also expressed concern that requiring Class A companies to use external parties to fulfill the risk assessment requirement and annual audit requirement may result in external parties performing a review of

the same cybersecurity program. The commenter recommended using the independent risk assessment expert to satisfy the annual audit requirement.

Some commenters suggested covered entities conduct risk assessments internally and use external consultants and service providers for other purposes for covered entities' cybersecurity/information security programs. A commenter indicated covered entities should have discretion to use external resources for their information security programs. Further, another commenter suggested the Department acknowledge the three lines of defense, including the third line of defense and allow the insurer to determine the type of expert (internal or external) to use for a covered entity's cybersecurity program.

With respect to the frequency to review and update a covered entity's risk assessment, a commenter suggested covered entities be provided flexibility. Another commenter suggested Class A companies review and update a risk assessment in the same manner as other companies and suggested risk assessments be "reviewed and updated annually and whenever a change in the business or technology causes a material change to the covered entity's cyber risk" as described in § 500.9(c). Another commenter requested that a Class A company have the option of conducting a risk assessment internally on an annual basis rather than using an external expert to conduct one triennially.

Commenters also suggested the Department provide clarification on the term "expert" or otherwise define this term. One commenter noted it may be helpful to provide a definition so the Department may feel comfortable allowing internal and external experts. This commenter also requested the Department provide examples of the type of certifications, education, experiences, or standards that may fulfill the expert requirement. Commenters requested clarification and guidance on the external expert's role, such as whether the external expert would conduct or review the risk assessment and raised questions regarding whether covered entities could partner with external experts to conduct the risk assessments.

Moreover, a commenter asked the Department to clarify that the scope of the annual risk assessment or triennial risk assessment does not involve an end-to-end review or review of each technical component. The commenter recommended that continual updates satisfy the annual risk assessment requirement so long as each technical component is considered during the three-year period. Another commenter stated there were several obligations under the regulation that are "based on a risk assessment", such as § 500.9(d), where covered entities need to understand the deliverable since the form is not clear. The commenter asked for clarification on the deliverable in the definition or provisions. Moreover, the commenter asked that the Department reconsider the scope and use of an external expert if the external expert requirement remained in the regulation.

Response: Based on its analysis of comments received, the Department understands the industry's concerns and removed § 500.9(d). Thus, questions regarding risk assessments performed by external experts or the role of experts no longer require clarification.

Comment: Several commenters wanted clarification on the types of third party certifications that would satisfy the requirements in § 500.9, such as System and Organization Controls ("SOC"), or those from HITRUST or the International Organization for Standardization ("ISO"), and whether existing frameworks, methodologies or standards may be used. Another commenter suggested exempting companies that already have one of these certifications from these requirements.

Response: The Department does not endorse or recommend any particular certifications. Covered entities must determine, in accordance with their risk assessment, whether particular certifications, frameworks, methodologies and standards would be appropriate for their needs and would comply with the requirements contained in Part 500. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter stated that § 500.10(a)(2) and § 500.10(a)(3) are redundant and requested these provisions be streamlined or that § 500.10(a)(3) be clarified to set out the level of verification required and specify the type of evidence necessary.

Response: The Department did not make any changes in response to this comment because they did not relate to a change proposed in the amendment, and the Department believes they are distinct and important.

Comment: Several commenters requested either that the Department restore deleted § 500.11(c), or that the Department confirm that this is a non-substantive change.

Response: The deletion of § 500.11(c) was a non-substantive change because it was duplicative of §500.19(b). Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter stated that § 500.19(b) is unclear and it was ambiguous if agents were only exempt to the extent covered by the principal's systems.

Response: It was not clear to the Department if this commenter was requesting a change to § 500.19(b). An agent, who is itself a covered entity, is exempt from Part 500 if such agent is covered by the cybersecurity program of another covered entity. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters also stated that there was no requirement for policies and procedures required by § 500.11 to be reviewed at least annually or regularly and that periodic assessments were insufficient and suggested continuous monitoring of TPSPs, that businesses should not be compelled to conduct annual assessments of third parties who they use just once every two years, and that the notice requirements in § 500.11(b)(3) be qualified by materiality and limited to successful breaches of the TPSP.

Response: Policies and procedures required pursuant to § 500.11(a) must be based on the risk assessment of the covered entity and address, to the extent applicable, "periodic assessment" of such TPSPs based on the risk they present and the continued adequacy of their cybersecurity practices. The requirement for periodic assessments based on the risk assessment means that some TPSPs will be reviewed more frequently than annually and some less frequently than annually. The Department does not believe that adding a new requirement for continuous monitoring of TPSPs is appropriate at this time.

Each covered entity must maintain policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, TPSPs, and such policies and procedures must include relevant guidelines for due diligence and contractual protections, including to the extent applicable, notice to be provided to the covered entity in the event of a cybersecurity event. Each covered entity must implement policies and procedures and include, to the extent applicable, the types of notices such covered entity requires from the TPSPs it engages. Covered entities are free to determine, based on their risk assessment, the scope of the notifications they require from their TPSPs, and how to comply with their Part 500 obligations, including the requirement in § 500.17 to provide notifications to the Department of certain cybersecurity events at TPSPs.

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

Comment: Commenters had other suggestions with respect to § 500.11, such as recommending that the Department directly regulate TPSPs, directly addressing how "non-traditional" third parties, such as agents and brokers should be handled, making the requirements risk based, and requiring TPSP policies and procedures contain continuous monitoring, security ratings and metrics requirements, along with an independent audit to identify specific third party risks. One commenter stated that vendor management is critical as entities must ensure service providers are operating within the requirements of the regulation but did not propose any specific changes be made.

Response: The Department agrees that vendor management is important. The requirements for TPSP policies and procedures contained in § 500.11 were unchanged in the amendment. Section 500.11 requires that TPSP policies and procedures be "based on the risk assessment." Covered entities are free to incorporate additional requirements if they deem it appropriate. Continuous monitoring, security ratings, metrics and independent audits may not be appropriate for every TPSP engaged by a covered entity.

To the extent a TPSP is a covered entity, that TPSP would be subject to the provisions of Part 500 applicable to such TPSP. If any agents, brokers, and other third parties are themselves covered entities, then they would be subject to the provisions of Part 500 applicable to them. If such parties fall within the definition of "third party service provider" under § 500.1 and such parties provide services to a covered entity, then the covered entity must comply with all Part 500 requirements with respect to TPSPs, including those requirements in § 500.11. The Department declines to further expand the scope of covered entities to include TPSPs or to further expand the scope of the definition of "third party service provider" at this time.

Therefore, the Department is not making any changes in light of these comments.

Comment: One commenter stated that the Department should require phishing-resistant MFA for privileged accounts in line with recent guidance from the White House, CISA, and the Consumer Financial Protection Bureau ("CFPB"). According to this commenter, the current proposed language conflicts with language on MFA from the Department's investigation reports and guidance from CFPB and CISA and these reports noted there were problems with using app-based MFA and encouraged the use of physical security keys. This commenter further mentions that NIST's refreshed Digital Identity Guidelines (SP 800-63) will include language to differentiate phishing-resistance authentication from legacy MFA tools that are susceptible to phishing.

Response: The Department encourages all covered entities to adopt phishing-resistant MFA where appropriate. Although physical security tokens, such as personal identity verification ("PIV") cards and security keys, offer phishing resistance, the Department believes it will be too costly and burdensome at this time to require only phishing-resistant MFA for all covered entities. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter stated that the requirement that the CISO approve MFA compensating controls in § 500.12 supports the need for the CISO to be independent because a CISO cannot be sourced from an existing provider that would be assessed and monitored. This would be of particular note in smaller firms where the entity

may have to manage multiple levers to retain providers they need to be able to stay in business and still improve their cyber posture under the scrutiny of an independent CISO.

Response: This comment was not clear to the Department and appears duplicative of other comments regarding whether a CISO should be independent previously discussed. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the Department reinstate § 500.12 as an exempted provision for those entities that qualify for a limited exemption pursuant to § 500.19(a), provide different requirements for "micro-sized entities," or explain why § 500.12 was removed because micro-sized companies do not routinely provide the types of access anticipated by this section of the regulation. This commenter argues that the amendment reflects no consideration of the fact that the majority of licensed mortgage companies do not operate with the same customer access functions or provide services that truly require such added security.

Response: This commenter may misunderstand the requirements contained in § 500.12 to only apply for customer access. The MFA requirements contained in § 500.12 apply for all situations specified by § 500.12, regardless of whether such access is made by a customer or an employee or other non-customer. MFA has been proven to be an effective mechanism to stop many types of attacks, as explained by Department-issued guidance, and implementation has become relatively simple and oftentimes free as part of the services purchased. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter stated that requiring MFA on all systems instead of only systems at greatest risk of exposing personally identifiable information ("PII") or interrupting business operations, is challenging.

Response: Limiting the MFA requirements to only those systems at greatest risk of exposing PII or interrupting business operations would not achieve the goals the Department intends with this provision. Even a compromised "low risk" internal workstation could pose an extremely high risk to other internal systems, to the

extent that comprised system could be leveraged to gain further access to such other internal systems. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter requested that the MFA requirements be updated to follow zero trust principles, and these controls be required regardless of whether the user is external or internal to a covered entity's location, and regardless of whether the application and data reside in a covered entity's data center or in a cloud platform as part of a software as a service ("SaaS") application.

Another commenter suggested aligning the MFA requirements in this section with the MFA requirements contained in the FTC Safeguards Rule to avoid duplicative requirements, or to address MFA in guidance instead of including as part of this amendment.

Several commenters requested to limit the scope of the MFA requirement for privileged accounts in § 500.12(b)(2), such as by excluding third party accounts, limiting to accounts that have access to information systems or data, or removing service accounts from the definition because it would not be possible to achieve and the CISO would have to annually approve compensatory controls. They also asked how entities without CISOs relying on a limited exemption pursuant to § 500.19(a) could approve compensating controls.

Response: The FTC Safeguards Rule requirement in 16 C.F.R. § 314.4(c)(5) would effectively require MFA in all instances because that provision requires MFA for any individual accessing any information system, unless the qualified individual responsible for overseeing the information security program and enforcing the information security program approves reasonably equivalent or more secure access controls.

Similarly, following zero-trust principles would effectively require MFA in all instances on all systems.

In response to these comments, the Department is revising § 500.12 to require that MFA be utilized for any individual accessing any of the covered entity's information systems, unless the covered entity qualifies for a limited exemption pursuant to § 500.19(a), in which case MFA must be utilized for remote access to the covered entity's information systems, remote access to third party applications, including but not limited to those that are

cloud based, from which nonpublic information is accessible, and all privileged accounts other than service accounts that prohibit interactive login. If the covered entity has a CISO, the CISO may approve in writing the use of reasonably equivalent or more secure compensating controls, and such controls must be reviewed periodically, but at a minimum annually.

The decision whether to implement compensating controls must be made by a CISO and accordingly entities making this decision will be required to have a CISO. All entities with relatively common information systems should be able to enable MFA for all instances described in this revised language, and those with more complicated information systems would benefit from having a CISO, in particular to approve compensating controls in certain instances where necessary and warranted.

Comment: One commenter suggested that the Department replace "may" with "shall" and "or" with "and" in § 500.12(a).

Response: The Department agrees with this comment because MFA is now required for all covered entities but does not believe that § 500.12(a) is necessary anymore. Therefore, the Department is deleting the requirement in § 500.12(a).

Comment: One commenter stated that § 500.12 presumes that all covered entities have a CISO and that covered entities entitled to the § 500.19(a) limited exception are not required to have a CISO.

Response: The proposed revisions to § 500.12 referenced above would require covered entities with a §500.19(a) limited exception to utilize MFA for the instances described in § 500.12, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls. Many covered entities relying on a § 500.19(a) exemption do not need to have a CISO and can satisfy the § 500.12 MFA requirements. Those covered entities that cannot implement MFA typically have more complicated systems where having a CISO would likely be warranted. Therefore, the Department did not make any changes in light of this comment.

Comment: One commenter stated that MFA for remote access to third party applications may not be feasible and recommends maintaining a risk-based approach. Another commenter stated that requiring MFA for remote access to third party applications would pose an extreme burden, as companies would potentially have to terminate relationships with third party vendors that do not use MFA, and the Department should only require MFA for remote access to third party applications where reasonable and available.

Response: For third party applications where MFA is not available or where implementing MFA would pose an extreme burden, § 500.12 permits the CISO to approve in writing reasonably equivalent or more secure compensating controls. Covered entities may also wish to seek to explore alternatives where the third party applications they utilize do not offer MFA or where implementing MFA can only be done so with extreme burden, as there are likely other third parties offering the same service where MFA can be implemented easily. Therefore, the Department did not make any changes in light of this comment.

Comment: With respect to § 500.12, one commenter requested clarification as to whether "remote access" means internal networks from external networks.

Response: Remote access includes both internal networks from external networks and external networks from internal networks. For example, § 500.12 requires MFA for "remote access to third party applications, including but not limited to those that are cloud based…." MFA is required even when accessing those third party applications from the covered entity's offices. Therefore, the Department did not make any changes in light of this comment.

Comment: With respect to § 500.12, several commenters suggested changes to limit the scope of the MFA requirement, such as basing it on a risk assessment, allowing covered entities to make security decisions based on the sensitivity of data that needs to be protected, or focusing the requirement on employees by modifying the language so it relates to the covered entity's personnel. Other commenters requested that the Department permit feasibility to be considered, similar to the requirements in § 500.15(a).

Response: The Department believes that the MFA requirements in § 500.12 are important to a covered entity's overall cybersecurity posture. All access should be secured, not just access by personnel. Access by vendors, contractors, and other external parties to the covered entities systems also pose a security risk. There are instances where MFA is technically feasible, but the covered entity, with the CISO's written approval, has opted for a reasonably equivalent or more secure compensating control. Therefore, the Department did not make any changes in light of these comments.

Comment: One commenter suggests deleting the "cloud-based" example because it is unnecessary and §500.12(b)(2) broadly encompasses third party applications. This commenter also states there are several instances of the phrase "including but not limited to" and none of these instances specifically identify a type of technology. Another commenter stated that it is generally unusual for the CISO to review MFA controls.

Response: The Department wants to specifically highlight the cloud-based example in this instance, and the CISO, as a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program, is in the best position to review these controls and authorize any exceptions. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters stated that the asset inventory requirement in § 500.13(a) is too burdensome because of, for example, the additional work and details required and suggested that it be based on a risk assessment as it would achieve an appropriate cost-benefit outcome, particularly given the speed and volume at which assets are developed and modified for many covered entities, or that the asset inventory only be required to be maintained "materially" in accordance with written policies and procedures. One commenter stated that, because the requirements in § 500.13 are very prescriptive, certain "micro companies" should be considered for exemption, or specific requirements should be included for these micro companies here. Other commenters requested clarification on what assets need to be included as part of an asset inventory or recommended that the Department require an asset inventory only for assets that contain or access nonpublic information. One

commenter suggested that IoT should be carved out from asset management because, for example, connecting any IoT device to an organization network should require prior approval from a designated information security office.

Response: The Department has determined that no change is necessary. Maintaining an asset inventory is a critical part of identifying assets that need to be protected. Pursuant to § 500.13(a), the asset inventory related policies and procedures must be part of the cybersecurity program, which is based on a risk assessment. Material compliance with the asset inventory requirements is insufficient. All assets that are included in the risk assessment must be inventoried, not just those that are material or that contain nonpublic information. Additionally, entities of all sizes must maintain an up-to-date asset inventory, and if a company is small, it should have fewer assets that need inventorying. To the extent an IoT device is covered by the cybersecurity program, it must be included as part of the asset inventory. The Department provides a free asset inventory template on the Department's website, the Cybersecurity Resource Center, for small and medium-sized companies.

Comment: Commenters asked for clarification regarding which business function is responsible for asset inventory, the IT Department or the CISO/Information Security Department. One commenter stated that the CISO should not be responsible for all asset management, but only cyber portions. One commenter asked the Department to consider replacing "recovery time requirements" with recovery time objective ("RTO") or recovery point objective ("RPO") because organizations use RTO and RPO values to calculate the cost of a cyber event.

Response: The Department is revising the first sentence of § 500.13(a) to clarify that the asset inventory is an inventory of the covered entity's information systems and is revising "recovery time requirements" to "recovery time objectives," which is the term NIST uses.

Comment: Commenters stated that certain requirements in the amendment are too prescriptive or should be based on the risk assessment, such as § 500.14(a)(2), with respect to controls that protect against malicious code,

and § 500.14(b), with respect to certain tools that Class A companies must implement and would mandate an outcome rather than requiring a process to be implemented.

Response: Controls are very helpful in mitigating risk, but controls can never guarantee 100% success. With respect to § 500.14(b), the amendment requires covered entities to implement an endpoint detection and response solution ("EDR") and a solution that centralizes logging and security event alerting ("SIEM") but does not require that these controls prevent all cyberattacks. With respect to § 500.14(a)(2), the Department is revising the language to explicitly state that the requirement is to "implement risk-based controls designed to protect against malicious code, including those that monitor and filter web traffic and electronic mail to block malicious content…." Furthermore, the requirement is not too prescriptive as no specific methodology is required, only that controls be implemented to protect against malicious code, including email and web filtering. Moreover, these requirements must be implemented as part of the cybersecurity program, which is based on a risk assessment, so the extent to which an entity must monitor and filter web traffic is risk-based, and a covered entity can determine how much monitoring and filtering is necessary based on the results of their risk assessment.

Comment: Commenters requested the training requirements in § 500.14(a)(3) not have a minimum annual frequency or be based on a risk profile, citing labor shortages and stating that training does not make sense for all personnel every year.

Response: The cybersecurity awareness training required for different personnel will vary in an organization and depend on the function of such personnel, but all personnel must undergo certain training, as determined by the organization in accordance with its risk assessment and its cybersecurity program. The amendment did not introduce the training requirement but clarifies that the requirement for cybersecurity awareness training includes social engineering and must be performed on a periodic, but at a minimum annual, basis. The Department is removing the word "exercises" from the phrase "social engineering exercises" to clarify that the training requirement must include a social engineering component, but that exercises such as phishing email test

campaigns are not required for certain personnel. For example, certain personnel may not be provided email where certain email specific exercises would not apply for such personnel.

Comment: Commenters noted the new Class A requirements in § 500.14(b) addressing EDR and SIEM mandate that companies use specific products, which may be costly and challenging for some to implement and the requirement was unclear, and suggested the Department may be shifting away from a risk-based approach by having CISOs approve equivalent or more secure controls. They suggested the Department modify this requirement, such as by removing it or making it risk based, noting covered entities may not have the ability to install equivalent controls, and the requirement increases operational time, expense, and work and may be too costly, and that covered entities should have discretion with respect to the solution that covered entities use based on the covered entity's network and information security risks. A commenter noted that the provision did not indicate the systems or endpoints that required EDR.

Response: The Department declined to remove the provision since the Department is providing covered entities with flexibility to implement "reasonably equivalent or more secure compensating controls" with the CISO's written approval in lieu of EDR and SIEM, and the Department believes Class A companies have the resources to implement EDR as well as SIEM, which would enhance cybersecurity risk management practices. Thus, CISOs may not need to implement compensating controls very often. Moreover, there is still some discretion in what Class A companies can implement as the regulation imposes minimum standards but allows covered entities with discretion to determine what EDR solution and what SIEM solutions to use based on their specific risk exposures. Class A companies implementing EDR must determine the systems and endpoints to include in accordance with their risk assessment.

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

Comment: Another commenter suggested the Department clarify and provide expectations for certain requirements, such as § 500.14(b)(1), and suggested the regulation incorporate a definition for lateral movement.

Response: The Department believes that expectations are clear and determined it was not necessary to add a definition of lateral movement because this term is commonly understood in the cybersecurity industry. Any clarifying guidance issued in connection with the requirements contained in Part 500 will not affect the language of the amendment. Thus, the Department did not make any changes in light of this comment.

Comment: Some commenters suggested revising or further enhancing the requirements in § 500.14(b), such as by including extended detection and response ("XDR") solutions in addition to EDR, requiring that backups be analyzed, clarifying what information systems needed to be included and monitored by the EDR and SIEM solutions, requiring that the logs in the SIEM solution be reviewed regularly, and adding security control and retention requirements around the maintenance of these logs similar to how covered entities maintain nonpublic information.

Response: The Department concluded it was not necessary to include XDR in the regulation because §500.14(b) provides that the CISO can approve reasonably equivalent or more secure controls. The proposed language allows CISOs to deploy detection and response tools, other than EDR, including those that may be considered more advanced. The Department declined to add the additional suggested requirements from these commenters because Class A companies implementing EDR and SIEM must determine the data and information systems to include and review, and the maintenance, security controls and retention with respect thereto, all in accordance with their risk assessment. Thus, the Department did not make any changes in light of these comments.

Comment: With respect to § 500.14(b)(2), some commenters expressed concerns regarding the logging system. One commenter noted some logging systems may not provide centralization or centralization may not be practical in some situations or may not be technically feasible. Another commenter asserted that centralized

logging may not be the best available method and may become less useful in the future because there are other platforms that provide real-time information. The commenter also noted that "centralized logging and security event alerting" is a prescriptive requirement. Another commenter asserted a "one size approach" relating to centralized logging may pose challenges for some types of organizations, such as those in the communications sector, and recommended removing the requirement or limiting it to those systems that support financial services regulated by the Department. Another commenter noted the language in § 500.14(b)(2) may be inadequate if logs from systems containing the most sensitive information are excluded. See NIST publication SP 800-92 providing that "organizations should require logging with the greatest importance…"

Response: Depending on the SIEM solution, certain systems may or may not be supported and it may not be practical in some situations or technically feasible. Class A companies implementing the requirements in §500.14(b)(2) must determine the systems to include, in accordance with their risk assessment. Thus, the Department did not make any changes in light of these comments.

Comment: Several commenters wanted to decide what types of nonpublic information they should encrypt, such as encrypting information based on their risk assessment or based on what management decides. Another commenter questioned whether § 500.15 required encryption for data in use, in addition to encryption for data in transit and data at rest. Other commenters expressed concern saying this would require significant resources or cause undue burden and expense, such as when encrypting commercial contracts, or when encrypting information on legacy systems.

Response: Section 500.15(a) requires encryption of "nonpublic information" held or transmitted by the covered entity both in transit over external networks and at rest. There is no requirement in § 500.15 to encrypt data in use. The term "nonpublic information" is defined in § 500.1 and includes certain information concerning individuals or derived from a healthcare provider, as well as business information where the tampering with, or unauthorized disclosure, access or use of, such information would cause a material adverse impact to the business,

operations or security of the covered entity. Business information rising to the level of nonpublic information should be encrypted. The Department does not believe that most customer contracts and other routine types of business information would rise to this level.

Furthermore, there are numerous free or low-cost encryption solutions available that make encryption a feasible solution in most situations. In many cases, widely used software and hardware have built-in encryption capabilities. Therefore, the Department did not make any changes in light of these comments.

Comment: Two commenters stated that they have relied on data-loss prevention solutions and secure transmission channels to protect data, and that effective compensating controls for encryption in transit over external networks may exist in the future. As a result, they requested the deleted language be restored from §500.15(a). Another commenter stated that compensating controls for encryption of data at rest should be based on more than feasibility because there may be compensating controls that make encryption unnecessary but did not provide examples of such compensating controls. According to another commenter, some regulatory agencies and courts may not allow for encryption for the data they receive.

Response: These amendments are designed to reflect the current and reasonably foreseeable cybersecurity environment. It would be impossible to design for all compensating controls that may one day exist.

Data-loss prevention solutions prevents data from being sent, and § 500.15(a) requires encryption of nonpublic information that is actually sent and is therefore not blocked from being sent. If secure transmission channels encrypt the communication being sent, that would satisfy the encryption requirements.

The Department is unaware of any regulatory agencies or courts that require nonpublic information be transmitted electronically only in unencrypted format and that would refuse to accept encrypted file attachments.

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

Comment: A commenter was concerned the language in § 500.16 was overly prescriptive, noting processes should be developed by covered entities rather than included in the regulation if the Department believes covered

entities should conduct programs based on risk assessments. Another commenter was concerned the response provisions were too broad and cited § 500.16(a)(v) as an example since it requires "the remediation of any identified weaknesses in information systems and associated controls." The commenter noted it did not allow covered entities to manage risk and threats based upon priority. Another commenter suggested the Department define the types of weakness requiring remediation as all information systems contain some level of weakness that cannot be remediated and recommended changing the language to reflect specific weaknesses.

Response: The Department is committed to ensuring that covered entities have adequate written incident response plans in place. Similarly, the SEC is proposing amendments to its Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Customer Information that would require brokers and dealers, investment companies, and investment advisers to adopt written policies and procedures for incident response programs that are reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. With respect to Section 500.16(a)(v), the remediation of weaknesses depends on several factors, such as risk assessments, specific circumstances relating to covered entities, types of weakness and how weaknesses relate to the covered entity's business and maintenance of nonpublic information. The Department understands that when covered entities determine their remediation plans for weaknesses, they will consider the degree of risk and threats and prioritize them. Therefore, the Department did not make any changes in response to these comments.

Comment: Commenters expressed concerns regarding the use of the terms "disruptive event" in §500.16(a) since the term is not defined, is not clearly described in the regulation, and could include events that are not cybersecurity events. Commenters suggested clarifying or deleting disruptive events so plans would be limited to cybersecurity events.

Response: In response to these comments, the Department revised § 500.16(a) to require covered entities "establish written plans that contain proactive measures to investigate and mitigate cybersecurity events" and not

use the term "disruptive." However, the Department determined that it was not necessary to revise the last sentence of § 500.16(a)(1) that required such plans to address "different types of cybersecurity events, including disruptive events such as ransomware incidents" because this phrase is already limited to cybersecurity events. The Department concluded covered entities should have plans that explicitly address ransomware attacks as described in guidance released by the Department in June 2021.

Comment: A commentator suggested "down chain critical parties" required for resilience should be included in the testing of the incident response plan in § 500.16(d) and in § 500.16(e) where cloud or hardened equipment may pose issues. Additionally, this commenter suggested including "identification of alternate communication and payment systems."

Response: The Department has determined it will not require entities to identify all downstream parties pursuant to the BCDR requirements in § 500.16(a)(2). Covered entities may decide to impose additional requirements on their third parties in accordance with their risk assessment and their TPSP policies and procedures. It is unclear to the Department what "identification of alternate communication and payment systems" means. Pursuant to § 500.16(a)(1), incident response plans must be designed to promptly respond to, and recover from, any cybersecurity event materially affecting the continuing functionality of any aspect of the covered entity's business or operations, and if identification of alternate communication and payment systems is important to a covered entity, in accordance with its risk assessment, then it may be appropriate for such covered entity to include as part of its incident response plan. Each covered entity must decide, in accordance with their risk assessment, what to include, but at a minimum must address the requirements specified in §500.16(a)(1). Therefore, the Department did not make any changes in light of this comment.

Comment: A commenter was concerned that the scope of the incidence response plan and business continuity management is not limited to those that are cybersecurity related. The commenter asserted the CISO should not be principally responsible for plans/programs for which others are responsible within the organization

or certify to matters that are not related to cybersecurity and suggested the expanded program would make the CISO responsible for plans/programs that that fell outside of the CISO's responsibilities. The commenter also suggested to the extent continuity and recovery are part of a cybersecurity program, the Department limit the continuity and recovery parts of the program to those that arise from cybersecurity issues.

Response: The Department has revised the language in the first paragraph of § 500.16(a) to limit the scope of incident response plans to cybersecurity events. Additionally, § 500.16(a)(2) was changed to limit the scope of business continuity plans to cybersecurity related disruptions.

Comment: One commenter asked for flexibility in § 500.16 based on the individual governance structures of insurance groups to allow insurers to oversee and manage incident response and business continuity and disaster recovery ("BCDR") plans at the group level and to make them applicable to the covered entities in their group.

Response: Covered entities that do not maintain their own cybersecurity program are permitted to meet the requirements of Part 500 by adopting all or a portion of the cybersecurity program maintained by an affiliate, including their incident response and BCDR plans. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters pointed out the significance of conducting a post-mortem after an incident occurs to make enhancements and address weaknesses and requested that determining the root cause and scope of a cybersecurity event be added as an additional core cybersecurity function of the cybersecurity program in § 500.2. Other commenters suggested additional items be included in incident response and BCDR plans, such as explicitly addressing advanced persistent threats, incorporating provisions with respect to local and federal law enforcement agencies, and requiring response teams to hold certifications.

Response: The Department agrees that determining root cause would be important as part of an incident response plan and is adding a requirement to § 500.16(a)(1) that incident response plans include preparing a root

cause analysis that describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence. The additional suggested items to include in incident response and BCDR plans may be appropriate for certain covered entities but it would depend on their risk assessments, and therefore the Department declines to add additional prescriptive requirements with respect to incident response and BCDR plans at this time.

Comment: With respect to backups in § 500.16(a)(1)(vii), a commenter expressed concerns about restricting recovery to backups since they could be compromised and noted there are various forms of recovery based on "the event and architecture." The commenter suggested replacing the language "from backups" with "methods and procedure."

Response: The Department did not change the language because covered entities should have plans to recover information from backups.

Comment: Commenters suggested the Department consider changing the frequency of the testing. One commenter proposed the Department offer flexibility and allow covered entities to conduct tabletop exercises with senior officers "regularly" or "every twenty-four months" under § 500.16(d)(1) and § 500.16(d)(2). Another commenter indicated that it would be challenging for covered entities to comply with annual testing due to the coordination of personnel and senior officers and recommended revising the timeframe to a biennial or two-year requirement for better compliance.

Response: The Department did not change the timeframe because the Department believes covered entities should test their incident response plans at least annually given the cybersecurity threat landscape.

Comment: With respect to § 500.16(d), one commenter suggested changing the term "test" to "exercise" noting the terms are closely related but may be distinguished in the information technology context. The commenter suggested the terms vary when identifying deficiencies in plans and procedures relating to cybersecurity.

Response: The Department declines to change the term from "test" to "exercise" in the amendment because the Department does not believe this is necessary.

Comment: Some commenters stated it was not necessary for the highest-ranking officer or other senior officers to participate in testing of the BCDR plan or incident response plan. Some commenters opposed CEO participation in exercises in the BCDR plan or in incident response testing because, for example, it would be administratively difficult and divert the CEO's attention from risk management. Commenters also noted senior officers and the CEO should not be mandated to attend all exercises. One commenter acknowledged that C-suite employees typically participate in tabletop exercises "as needed" or when "appropriate" but noted the highest-ranking executive does not need to be involved with all components of the annual testing of the incident response plan in detail and the inclusion of the highest-ranking officer could lead to inefficiencies.

Commenters suggested covered entities should have flexibility with respect to the required participants for testing. One of the commenters suggested changing the language to allow covered entities to determine the proper individuals required to participate instead of mandating specific participants. Another commenter suggested the Department modify "key staff that would be involved in the actual incident response scenario, including to the extent applicable, senior executives" should be required to participate.

Response: The Department declined to remove the requirement that senior officers, including the highest-ranking officer, participate in the testing of incident and BCDR plans. There is an evolving cybersecurity threat landscape and senior officers, which includes the highest-ranking officer, and staff critical to respond to a cybersecurity incident must be aware of the actions they will take in the event of a cybersecurity incident. The Department acknowledges that the CEO does not need to be involved in all of testing or participate in all of the exercises.

Comment: Several commenters expressed concerns that the BCDR requirements in § 500.16(a)(2) went beyond cybersecurity, were confusing, complex, and prescriptive. In addition, commenters noted BCDR

requirements included certain terms, such as "backup", that were unclear, and recommended plans be limited to ensure the availability and functionality of material services or restoration of operations to a viable level. Moreover, commenters suggested that CISOs should not be responsible for the entire BCDR plan that covers more than cybersecurity as various experts within the organization are responsible for different aspects of BCDR, BCDR is managed enterprise-wide, and CISOs should not be required to certify compliance for areas outside the CISO's responsibilities. The commenters' suggestions included removing the BCDR requirements in their entirety, limiting the BCDR requirements to cybersecurity-related events and removing the enumerated minimum requirements of BCDR described in §§ 500.16(a)(2)(i)-(vi). A commenter also suggested qualifying § 500.16(a)(2) with a reasonable effort standard noting it is not practical for a covered entity to guarantee the availability and functionality of its services. In contrast, another commenter suggested expanding the use of the term "disaster recovery" and enhancing certain requirements contained in § 500.16(a)(2)(i)-(vi).

Response: In response to these comments, the Department is: (a) revising the language § 500.16(a)(2) to state that BCDR plans must be designed to ensure the availability and functionality of "the covered entity's information systems and material services and protect the covered entity's personnel, assets and nonpublic information in the event of a cybersecurity-related disruption"; and (b) modifying the language in § 500.16(a)(2)(iv) to reference "critical data and information systems" instead of "data and documentation." The Department believes that the minimum requirements of BCDR described in §§ 500.16(a)(2)(i)-(vi) are important and should be included in the BCDR plan. The Department also revised these subsections to focus on cybersecurity-related matters and the covered entity's information systems, but declined to expand, enhance or otherwise modify these minimum requirements for the BCDR plan. Additionally, under §500.16(a)(2), covered entities are required to establish a BCDR plan that is "reasonably designed to ensure the availability and functionality" but is not required to guarantee any particular outcomes.

Comment: Commenters stated requiring covered entities to distribute plans to "necessary" employees is vague, may be impractical or complex, and may present challenges, such as with respect to security. Commenters suggested covered entities be permitted discretion on how they handle access to, and distribution of, such plans; that employees who receive plans described in § 500.16(b) and participate in testing under §500.16(d) be limited to staff critical to the response; and that covered entities should determine the appropriate personnel. Additionally, another commenter suggested certain necessary third parties be included as part of the testing requirements under § 500.16(d).

Response: Current copies of the plans or relevant portions therein must be distributed "or otherwise made accessible" to all employees necessary to implement such plans in accordance with § 500.16(b). To the extent such plans are not distributed, they must be made accessible, including during a cybersecurity event. The Department believes that all employees necessary to implement such plans would be critical to any response, and covered entities must determine who such necessary employees are to implement the various requirements in such plans. To the extent certain third parties are necessary for the resilience of the covered entity's operations, covered entities may deem it appropriate to involve them in any testing efforts and covered entities may determine, in accordance with their risk assessment, to include provisions with respect to third parties as part of their plans. The relevant employees at the covered entity who are responsible for overseeing and managing such third parties would also need to be involved and aware of the third parties' involvement and have access to current copies of the plans or relevant portions therein. The Department is revising § 500.16(d) by removing paragraph (2) with respect to the BCDR plan and revising paragraph (1) to state that testing includes the "incident response and BCDR plans with all staff critical to the response, including senior officers and the highest-ranking executive at the covered entity…." With respect to testing, the Department believes that senior officers and the highest-ranking executive at the covered entity are necessary and such persons are critical to the response.

Comment: Several commenters requested clarification with respect to the backup requirements in §500.16, stating that it was unclear what information or systems needed to be backed up or what qualifies as a backup, and that it would be burdensome to backup all facilities, systems, and infrastructure. Recommendations included adding a materiality threshold, allowing for "equivalent technologies", such as replication or limiting the requirement to apply to key data, information systems essential to a covered entity's operations, or data necessary to ensure the availability and functionality of the covered entity's services.

One commenter requested the BCDR requirements in § 500.16 be aligned with requirements from other regulatory bodies, such as federal banking agencies and global banking regulators, and requirements from the Federal Financial Institutions Examination Council ("FFIEC").

Another commenter recommended backups be restricted to those connected to "cybersecurity issues."

Response: In response to these comments, the Department modified the language in § 500.16(e) to provide that "covered entities shall maintain backups necessary to restoring material operations." To the extent that "equivalent technologies" would satisfy the backup requirements contained in § 500.16, including storage of information offsite, being adequately protected from unauthorized alterations or destruction, and the ability to restore critical data and information systems, those technologies would qualify as backups. The amendment does not specify any particular technology to use to accomplish this. To the extent that replication only duplicates the current data and would also replicate corrupted or encrypted information following a ransomware attack, and restoration from an earlier unencrypted version is unavailable, then such replication would not satisfy the backup requirements in § 500.16. The Department also revised the language in § 500.16(a)(2)(iv) to state that covered entities' BCDR plans need to include procedures for the maintenance of back-up facilities, systems and infrastructure … to enable the timely recovery of critical data and information systems…." The Department also modified § 500.16(d)(3) to state that each covered entity must test its ability to restore its critical data and

information systems from backups. It was unclear to the Department how to restrict backups to those connected to cybersecurity issues.

Comment: Another commenter, with respect to § 500.16, suggested that covered entities may not need to maintain backups if they use cloud service providers.

Response: Covered entities using cloud service providers still need to maintain backups that are adequately protected from unauthorized alterations or destruction. Using cloud services does not guarantee the requisite protection from unauthorized alterations or destruction. Therefore, the Department declined to make any changes in response to this comment.

Comment: A commenter suggested offsite storage be deleted in § 500.16 as offsite storage has certain shortcomings, such as substantial time delays for restoring data and expanding potential attack surface.

Response: The Department believes it is important for BCDR plans to include procedures for storing information offsite, and covered entities are free to choose how best to accomplish this requirement in accordance with their risk assessments. Not all offsite storage options would involve delays in data restoration, such as immutable cloud storage services. To the extent physical media is sent to an offsite storage facility, any nonpublic information included therein must be encrypted or otherwise secured in accordance with the requirements in § 500.15. Covered entities can choose to store information in other places in addition to offsite, and the requirements in this provision are in line with recommendations from other governmental regulatory agencies. Therefore, the Department did not make any changes in response to this comment.

Comment: Several commenters suggested that companies be permitted to delay notifications pursuant to §500.17(a) in certain circumstances, such as when there are ongoing investigations. Commenters also requested that they be permitted to disclose, simultaneously, incidents to customers, law enforcement, and regulators.

Several commenters suggested reconsidering the changes to § 500.17 or stated that the notification requirements overall are overly burdensome on small businesses and requested the requirement be inapplicable in certain circumstances, such as when a third party's site is hacked.

Response: The timeframes specified for notifications under § 500.17(a)(1) should not be delayed for any reason as timely notifications are used by DFS to identify techniques used by attackers and enable DFS to respond quickly to new threats in order to protect consumers and the financial services industry. The Department agrees that covered entities do not need to report cybersecurity events in certain circumstances, including a hack of a third party's site, except when one of the other requirements in § 500.17(a)(1), such as having a reasonable likelihood of materially harming a material part of the normal operations of a covered entity, is also met. Therefore, the Department is removing§ 500.17(a)(3) and moving the reference to notifications regarding third parties to § 500.17(a)(1).

Comment: Several commenters request that the notification form for reporting cybersecurity events be published to ensure that covered entities understand the types and amount of information that should be prepared for submission.

Response: The notification form is already available on the Department's Portal. Anyone who wishes to view the notification form for reporting cybersecurity events can create a Portal account from the link on the Department's website and view what the current notification forms require, which includes text boxes where the filer enters a description of the cybersecurity event and the dates the cybersecurity event took place. Therefore, the Department did not make any changes in response to this comment.

Comment: One commenter stated that state data privacy and breach notification laws use the "without unreasonable delay" standard and permit 30-45 days to determine whether there was a data breach, and that it would be impractical to properly conclude whether the event is reportable within 72 hours. Several commenters requested clarification as to when the 72-hour reporting period begins, requested a longer period prior to

disclosure pursuant to § 500.17(a), or suggested that the notification clock only begin after completion of an initial forensic assessment. Other commenters requested additional time to allow for investigation and processing of the ransomware threats.

One commenter stated that longer-term vulnerability disclosure norms have emerged, such as where security researchers make a 90-day allowance following the discovery and reporting of a vulnerability in another vendor's software.

Response: The requirements in §§ 500.17(a)(1) & (c) are clear. Covered entities must notify the Department as promptly as possible but in no event later than 72 hours from a "determination" that a cybersecurity event has occurred and within 24 hours "of the extortion payment." The time period does not start during the initial "investigation and processing" stage, only following a determination that the cybersecurity event has occurred. Early reporting is important and should not be delayed until a forensic assessment has been completed, to the extent such forensics would exceed these reporting time periods. Covered entities are further required pursuant to § 500.17(a)(2) to provide follow-up information "regarding the investigation of the cybersecurity event" and "have a continuing obligation to update and supplement the information provided". DFS understands that the initial notification may only contain limited information.

Additionally, longer term vulnerability disclosure periods referenced by the commenter are not applicable to cybersecurity events where notifications must be provided to the Department, but rather to security research disclosures to software vendors or service providers so they can fix a reported vulnerability prior to a security researcher making their findings publicly known.

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

Comment: Several commenters requested streamlining notification requirements, such as by permitting notification forms of another regulator to be used for the purposes of § 500.17(a). Others suggested that reporting to the Department was duplicative of reporting to another regulatory agency and that it was burdensome because

these reports could be unrelated to a service regulated by the Department or to New York customers or may involve immaterial incidents. Other commenters requested that the notification requirements be limited to only apply where New York residents were impacted.

Response: The same information provided to other regulators will likely satisfy the notification requirements here, as the DFS Portal contains a text box requesting a description of the cybersecurity incident where the filer can copy/paste the same information already provided to another regulatory agency. Reporting to other regulators alone will not guarantee that the Department receives this information, and a breach of any customer's information is indicative of a possible security issue at the covered entity, regardless of where that customer resides.

Further, the materiality thresholds in § 500.17(a)(1)(ii) are clear that immaterial events do not need to be reported unless they were reported to another governmental body, self-regulatory agency, or other supervisory body; involved an unauthorized user gaining access to a privileged account; or resulted in ransomware deployment within a material part of the covered entity's information system.

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

Comment: Several commenters requested that "disrupting" and "degrading" be removed in § 500.17(a)(1)(ii) because these terms are overly broad and ambiguous and including them would result in unnecessary administrative burdens, including increased costs and demands on staff, and because they are not necessary.

Response: The Department agrees that "disrupting" and "degrading" are not necessary because a disruption or degradation upon any material part of the normal operation(s) of the covered entity would result in material harm to a covered entity, which is already captured by the requirements of § 500.17(a)(1)(ii). Therefore, the Department is deleting the terms "disrupting" and "degrading" in § 500.17(a)(1)(ii).

Comment: One commenter stated that §§ 500.17(a)(1)(iii) and (iv) should not be subject to a notification requirement unless they trigger one of the other criteria for an event requiring notification in § 500.17(a)(1).

Response: New § 500.17(a)(1)(iii) and (iv) refer to notifications where an unauthorized user has gained access to a privileged account and there has been a deployment of ransomware within a material part of the covered entity's information system, both of which are important events themselves that should require notifications. Therefore, the Department did not make any changes in light of this comment.

Comment: Several commenters suggested that § 500.17(a)(1)(iii) is too broad and would result in over-reporting by including all types of privileged accounts where an unauthorized user has gained access. Some suggested the scope only include where the account had access to nonpublic information or where there would be a material risk of harming, disrupting, or degrading a material part of operations, was for a prolonged period of time, was the result of a systemic issue, involved multiple privileged accounts, or otherwise materially impacted systems or data.

Response: In response to these comments, the Department is removing paragraph (2) of the definition of "privileged account" so that only unauthorized access to accounts that perform security-relevant functions that ordinary users are not authorized to perform are reportable events.

Comment: One commenter requested clarification regarding that the term "deployment" in § 500.17(a)(1)(iv) and whether thwarted ransomware attempts need to be reported. Other commenters stated that ransomware notification should only apply where ransomware has a material or significant impact on a covered entity's information system, such as where exfiltration of data resulted.

Response: Deployment of ransomware means that the ransomware program is installed or running on any of the covered entity's information systems. Thwarted ransomware attempts would not be reportable because the installation or execution was prevented. Not all ransomware involves exfiltration of data. Many instances of ransomware involve only encryption of files without exfiltration. Section 500.17(a)(1)(iv) limits notifications of

ransomware events to where it resulted in the deployment of ransomware within a "material part of the covered entity's information system." Adding an additional qualification is unnecessary. Therefore, the Department did not make any changes in light of these comments.

Comment: Several commenters requested clarification regarding the requirement to provide additional information in § 500.17(a)(2) and asked what information needed to be obtained and provided, and how the covered entity would prepare to comply with this section. Certain commenters recommended changing the provision, such as making it an obligation to respond to information requests from the Department or adding a materiality qualifier or reasonableness component or excluding information subject to investigation.

Other commenters requested limiting the continuing obligation to update and supplement information provided, such as to only information known and material to the facts, or when substantially new or different information becomes available.

Other commenters expressed concern regarding the 90-day timeframe and commented that it would be difficult or impossible to meet if requests were received close to that deadline.

Response: In response to these comments, the Department is revising § 500.17(a)(2) to remove the 90-day and website form references and require that covered entities promptly provide any information requested regarding the cybersecurity event. The information requested will be limited to information regarding the cybersecurity event, which is relevant, and the continuing obligation to update and supplement is limited to the information previously provided.

Comment: With respect to § 500.17(a)(3), several commenters requested either clarification on what "affected by" means or that a materiality qualifier be added. Certain commenters requested the language mirror the covered entity's own reporting requirements in § 500.17(a)(1)(ii) or a longer time period for reporting be provided.

Response: The types of notifications that the Department believes are important with respect to cybersecurity events at TPSPs are the same types of notifications described under §500.17(a)(1), such as cybersecurity events at TPSPs, where notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body, and cybersecurity events at TPSPs that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity.

For this reason and in response to these comments, the Department is deleting the requirement in § 500.17(a)(3) and revising § 500.17(a)(1) to clarify that the cybersecurity event notifications include incidents at the covered entity, its affiliates, or a TPSP. However, the Department believes that the current reporting time periods in § 500.17(a)(1) are appropriate and did not make any changes in that respect.

Comment: One commenter requested that the requirement to file certifications pursuant to § 500.17(b) be removed because the Department will soon be requiring insurance agents and brokers who are renewing their licenses to certify to Part 500 compliance.

Response: The Department has concluded that no change is necessary because all non-exempt covered entities must comply with the certification requirements under § 500.17(b), even if they are separately certifying for license renewal purposes.

Comment: Commenters requested that the section be revised to allow for a form of material compliance, provide that remediation during the year would not prevent a covered entity from submitting a certification of compliance, or state that certifications should be allowed if a covered entity is fully compliant at the time of certification and in material compliance during the prior calendar year.

Response: The Department has revised the proposed language to allow for material compliance by stating in relevant part that: "(a) certifies that the covered entity materially complied with the requirements set forth in this Part during the prior calendar year; and…."

Comment: One commenter requested that the Department allow administrative flexibility to enable assistants to submit the certification on behalf of others.

Response: The Department has determined that no change is necessary because there is already administrative flexibility. If an executive reads and "sign offs" on the certification, an assistant may perform the administrative task of submitting the certification via the DFS Portal.

Comment: One commenter suggested the Department introduce new technologies and methods of filing the forms required by § 500.17(b)(2).

Response: The Department prefers to receive the forms required by § 500.17(b)(2) via the Department's secure Portal and is therefore not making any changes in light of this comment.

Comment: One commenter stated that covered entities cannot ascertain whether they are compliant with Part 500 because the regulation has many undefined standards throughout.

Response: The Department concluded that no change is necessary because covered entities should know whether they are in compliance and any undefined terms are commonly used and understood and therefore do not need to be defined in Part 500.

Comment: One commenter stated that the proposed amendments could be interpreted to require regulated entities to provide DFS with documentation about their suppliers' confidential security practices to certify compliance.

Response: The Department concluded that no change is necessary because the proposed amendments are not requiring covered entities to provide documentation about suppliers, vendors, and other TPSP's security practices; rather, it requires that the written certification be based on, among other things, documentation of outside vendors and only "to the extent necessary."

Comment: Commenters requested that the Department clarify what data and documentation is sufficient to accurately determine and demonstrate full compliance.

Response: The Department has determined that no change is necessary because it believes the proposed amendments are clear as to what data and documentation is sufficient. The amendments list some examples of data and documentation "including…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…."

Comment: Commenters stated that the requirement in the proposal to document noncompliance and identify specific areas of vulnerability will create substantial cybersecurity risk and put the Department in possession of a list of prime targets for cyberattack or extortion, which bad actors will seek to access and exploit, and suggested that this requirement be removed. Commenters also stated that § 500.17(b)(1)(ii) is overly broad and burdensome because, for example, it requires the compilation and disclosure of detailed information that would normally be obtained through the examination process, and also asked for clarification whether, if there were deficiencies in cybersecurity compliance that have been remediated, they still must submit remediation plans and timelines. Commenters requested that a covered entity not be penalized for identified deficiencies as long as the entity is undergoing remedial efforts to address them and stated that the section may diminish a covered entity's flexibility to update remediation plans to account for changes to risk.

Response: The Department revised § 500.17(b)(1)(ii) to delete the requirement to submit an identification of all areas, systems and processes that require material improvement, updating or redesign, and the requirement to submit remediation plans, and revised § 500.17(b)(3) to require that these be retained by the covered entity for examination and inspection by the Department upon request.

Comment: Several commenters requested that the dual signatory requirement in §500.17(b)(2) was unnecessary. Certain commenters suggested other signatories, such as the senior governing body or another officer, or that the covered entity be the sole signatory. Other commenters suggested that only the highest ranking

executive sign, and requested that the Department remove the CISO as a signatory, that covered entities be given a choice of having either the CISO or the highest-ranking executive sign, or require that only the CISO signs.

Response: It is important to have both the CISO, as the person in charge of overseeing the cybersecurity program at the covered entity, as well as the CEO or other highest-ranking executive, as the person in charge of the business, sign and be involved with cybersecurity compliance. Therefore, the Department did not make any changes in light of these comments.

Comment: Commenters requested clarification regarding the certification and acknowledgement forms referenced in § 500.17(b) and requested that the revised forms include "to the best of their knowledge" language when they are signed by individuals. Commenters also expressed concerns that forms are no longer included in the amendment because introducing new requirements this way could, according to these commenters, violate the New York State Administrative Procedure Act ("SAPA"), such as with respect to the forms referenced in §500.17 and § 500.19.

Response: The forms referenced in the amendments will contain the substantive information set forth in Part 500. With regard to adding "to the best of their knowledge" language, the forms will contain substantially similar language as appears currently on Appendix A, which states "To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge …."

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

Comment: With respect to the requirement to notify the Department of an extortion payment made in connection with a cybersecurity event involving the covered entity pursuant to § 500.17(c), several commenters expressed concern and requested that the provision be deleted, that additional time be provided, that the provision be updated to ask instead for indicators of compromise or other incident-related information, or that an exception be provided where law enforcement is engaged and the covered entity has been instructed or encouraged to keep information confidential. Commenters stated that the notice timeframe was extremely short, that it was

inconsistent with CIRCIA, that it would affect covered entities' willingness to freely share information and potentially create conflicting obligations if they are working with federal authorities or other law enforcement agencies following a ransomware event. One commenter stated that the requirement to consult with the Office of Foreign Assets Control ("OFAC") could add significant time to the due diligence process with little benefit to a company's security and resilience.

Response: The notification requirement in § 500.17(c) is triggered following the payment itself, not when the incident occurs or is discovered. Presumably, at least some time has passed, and the entity has evaluated the situation and subsequently made the decision to pay the ransom. Section 500.17(c)(1) only requires notice of the payment, with additional details within 30 days pursuant to § 500.17(c)(2).

The notification requirement in § 500.17(c) aligns with the proposed regulations under CIRCIA, and deals with ransomware payments and the reasons companies made such payments. The Department may separately request indicators of compromise or other incident-related information during its follow-up investigation.

It was unclear to the Department what conflicting obligations will arise and when or if law enforcement or federal authorities would request companies not to report to the Department. This provision does not require consultation with OFAC before payments are made, only notice of the payment itself, and provides 30 days for the covered entity to provide a written description of all diligence performed to ensure compliance with OFAC and other applicable rules and regulations. The Department does not believe this to be a burdensome requirement.

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

Comment: Commenters requested clarification or deletion of the reference to certain terms used in §500.19, such as "independent contractor" and "affiliate."

Response: These terms were not introduced in the amendment as they are currently in Part 500 and the Department believes they are clear. Therefore, the Department did not make any changes in light of these comments.

Comment: Several comments requested changes with respect to § 500.19, such as increasing the gross annual revenue dollar threshold in § 500.19(a)(2), restoring § 500.12 as an exempted provision in § 500.19(a) because MFA is costly, and increasing the time in § 500.19(h) to comply after a covered entity ceases to qualify for an exemption. A commenter stated that the definition of "small business" adopted by Part 500 doesn't reflect the risks faced by "micro" businesses.

Response: The Department believes that the thresholds specified in § 500.19(a) are appropriate and additional categories are not necessary. Evidence suggests MFA is the best way to avoid many breaches and is currently cheap and easy to implement. Because Part 500 is based on a risk assessment, the requirement that smaller entities not covered by the exemption under § 500.19(a) implement a cybersecurity program is not unduly burdensome and ensures the safety and soundness of their information systems It also ensures their consumers receive adequate protection. However, in response to the comment requesting for the increase in time, the Department is changing the timeframe from 120 days to 180 days.

Comment: A commenter questioned whether Part 500 applies to or should apply to service contract providers because, according to this commenter, § 7903 of the Insurance Law exempts service contract providers from all provisions of the Insurance Law.

Response: Section 7903(a) of the Insurance Law provides that: "Notwithstanding any other provision of this chapter to the contrary, the marketing, sale, offering for sale, issuance, making, proposing to make and administration of service contracts by any provider, administrator or other person, shall be exempt from all other provisions of this chapter." The regulation is promulgated in relevant part pursuant to Article 79 and the Financial Services Law and § 7903 does not exempt service contract providers from requirements imposed by the Financial

Services Law and regulations promulgated pursuant thereto and Article 79, including Part 500. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters expressed opposition to the penalty provisions in § 500.20, such as by stating that the fines and penalty structure was unclear or that it should not be a violation of law to suffer an information security incident or otherwise be attacked by a criminal enterprise.

Response: The amendments merely set forth the factors the Department will take into account when deciding whether to impose a penalty under the Banking, Insurance, or Financial Services Laws. It does not impose penalties as those are set forth in the law. The requirements contained in Part 500 are designed to ensure that covered entities have a cybersecurity program in place and follow certain minimum standards and industry best practices to protect against a cybersecurity incident. If the requirements of Part 500 are met, then the covered entity is in compliance with Part 500 and the factors contained in § 500.20 would not be considered as penalties under the law would be inapplicable. Therefore, the Department did not make any changes in light of this comment.

Comment: Several commenters expressed concern regarding § 500.20(b) and suggested that this provision not be enacted or the 24-hour period extended to a longer period because, for example, it is broad, unclear, unduly punitive and inflexible, should have a scienter requirement, should base whether a violation has occurred solely on non-compliance with the requirements of Part 500 and not whether a breach has occurred. It also exposes covered entities to penalties for even brief noncompliance, does not provide time to rectify issues, is inconsistent with penalty calculations provided in other regulations issued by the Department, could impact a covered entity's financial stability, and does not take into consideration either the concept of layered security controls where a company expects and plans for individual control failures by having additional controls based on risk, or periodic reviews that identify gaps and needed updates.

Response: In response to these comments, the Department revised § 500.20(b)(2) to add a materiality qualifier so this provision now states: "the material failure to comply for any 24-hour period with any section of this Part." Material failures to comply with a 24-hour period would therefore constitute a violation. Further, the Department takes into account the factors specified in § 500.20(c), such as the good faith of the entity, in assessing penalties for violations. Moreover, a violation is not based solely on whether a breach occurred but also on whether the breach occurred because of a failure to comply with any of the requirements contained in Part 500.

Comment: One commenter requested an additional factor be added to § 500.20(c) to reflect the degree to which the covered entity has compensating controls.

Response: Compensating controls are specifically permitted in several provisions in Part 500 where the provision explicitly states so. The Department does not believe that compensating controls are appropriate where the provision does not explicitly state. Therefore, the Department did not make any changes in light of this comment.

Comment: Commenters had questions regarding the effective date of the amendments and when annual reporting requirements will begin, stating that nothing should change as the reporting requirement has been in place for five years.

Response: Pursuant to § 500.21, the amendments will become effective upon publication of the Notice of Adoption in the State Register. Pursuant to § 500.22(d)(1), covered entities have 30 days from this effective date to comply with the new requirements specified in § 500.17. The due date for the notice of compliance in §500.17(b) remains April 15 of each year. Therefore, the Department did not make changes in light of these comments.

Comment: Commenters stated that different transitional periods make compliance more complex and confusing and suggest harmonizing the transitional periods. One commenter requested that the Department delay

all compliance dates by at least one or more years as the FTC did due to concerns over the lack of qualified personnel.

Response: The various requirements under Part 500 will take different amounts of time for covered entities to implement. Provisions that require less time should be implemented sooner in order to improve the covered entity's cybersecurity. Therefore, the Department did not make changes in light of this comment.

Comment: Several commenters requested longer transitional periods for all parts, such as providing one or two more years due to reputational risks and legal risks associated with non-compliance, budgetary review processes, additional training for staff, the need to create or update policies and procedures, amend contracts, obtain approval from the board, or make appropriate upgrades. One commenter stated that the compliance dates are aggressive and will divert focus to non-material issues and reporting.

Commenters requested a longer transitional period for several provisions in the amendment, such as with respect to §§ 500.2(c), 500.3, 500.4, 500.5, 500.7, 500.9, 500.12, 500.13, 500.14, 500.15, 500.16, and 500.17. No commenters requested a shorter transitional period for any of the provisions listed in § 500.22(d).

Specifically, with respect to § 500.2(c), one commenter requested more time to allow for the implementation and review of controls related to third party engagement, such as contracts and sourcing.

With respect to § 500.3, one commenter requested more time to allow for larger organizations with many more policies to obtain the necessary approvals.

With respect to § 500.4, commenters stated more time is needed to allow for adjustments to be made to the reporting procedures, such as reporting requirements of the CISO, the annual reporting of the cybersecurity program, plans on remediating inadequacies, cybersecurity events, and more.

With respect to § 500.5, one commenter suggested a longer transitional period due to the significant increase in the scope required for penetration testing and the sourcing and contract needs for any third parties.

With respect to § 500.7, commenters requested more time to help ensure the implementation of all new requirements, especially for larger organizations. Commenters requested more time for § 500.7(b) to meet the new requirements for covered entities to identify a solution, test, architect it, and redesign applicable processes and services accordingly, for the broad application of this requirement across all platforms, and for challenges related to third party applications.

With respect to §§ 500.9(c) and (d), several commenters requested more time due to the new changes, the risk assessment review for Class A companies, associated budgetary changes, and to update their risk assessments.

With respect to § 500.12, one commenter stated they needed more time to evaluate solutions that will need to leverage compensating controls, obtain approvals, and deal with potential challenges with implementing required solutions to third party applications. Other commenters stated more time is needed for entities to reevaluate relationships with existing vendors, implement MFA and compensating controls where possible, and shift to alternative vendors if necessary, since due to associated costs and existing contracts, not all vendors are willing or able to implement MFA and renegotiating contracts may place covered entities in a poor bargaining position.

With respect to § 500.13, one commenter stated more time is needed since these requirements can be complex, time consuming, and difficult to implement.

With respect to § 500.14, one commenter requested more time due to the broad application of this requirement across all platforms, and for challenges related to third party applications.

With respect to § 500.15, one commenter stated more time is needed due to the increased scope and broader application of the encryption requirement.

With respect to § 500.16, one commenter stated more time is needed for covered entities to evaluate impacts of the new requirements and potential solutions required to comply.

With respect to § 500.17, one commenter stated companies need more time to implement the requirements before signing a certification or acknowledgement. Another commenter stated covered entities need much longer than 30 days to build processes and identify resources to capture events that are newly required as reporting obligations under §500.17, otherwise, it is possible the first certification that must be signed will be this year, leaving companies little room to prepare. Two commenters stated more time is needed to allow entities to create new procedures so information can be presented to the highest-ranking executive and that the executive would require more than 30 days to be able to review all material to confirm compliance with Part 500. Another commenter requested more time so that this section will go into effect for the 2024 attestation.

Response: In response to these comments, the Department is revising § 500.22(d)(2) by adding sections 500.4, 500.15, and the other subsections of 500.16 in addition to §§ 500.16(e) to 500.22(d) such that these provisions now have a one-year transitional period. The Department is revising § 500.22(d)(3) by adding the other provisions of § 500.7 and removing § 500.12 such that these provisions now have an 18-month transitional period. The Department is revising § 500.22(d)(4) by adding § 500.12 such that these provisions now have a two-year transitional period.

The Department did not make changes in response to the comments on § 500.2(c) and § 500.9 due to the removal of § 500.9(d) from the amendment. The Department declines to modify the transitional periods for the other provisions requested by these commenters because the Department believes those transitional periods are appropriate.