U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

August 14, 2023

Via cyberamendment@dfs.ny.gov

Joanne Berman
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: New York State Department of Financial Services; June 28, 2022, Revised Proposed Second Amendment to Regulation 23 NYCRR 500 (Part 500 or the Cybersecurity Regulation)

Dear Ms. Berman:

The U.S. Chamber of Commerce appreciates the additional opportunity to comment on the New York State Department of Financial Services' (DFS' or the Department's) June 28, 2023, revised proposed second amendment to regulation 23 NYCRR 500 (the amendment or the proposal), which governs cybersecurity requirements for financial services companies.[1]

The Chamber appreciates and values the effort that DFS leadership and staff made in developing its proposal and assessing stakeholder feedback. Alone, DFS' 92-page assessment of public comments (APC)[2] is an impressive work product. The Chamber continues to have concerns, however, and we respectfully submit these comments in a constructive and genuine attempt to achieve better policy outcome (see Appendix A).

[1] https://www.dfs.ny.gov/industry_guidance/cybersecurity
https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_text_20230628.pdf
https://www.dfs.ny.gov/system/files/documents/2023/06/2022.11.09_Bracketed_Underlined_SAPA_23NYCRR500_0.pdf
https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf

[2] https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_apc_20230628.pdf

Key Points

- Notwithstanding some welcome changes, DFS' June 2023 amendment to its cybersecurity regulation seems substantially similar to its November 2022 proposal.
- DFS and covered entities need to better partner to increase their joint cybersecurity objectives, including establishing safe harbor provisions in the cybersecurity regulation. Prescription without protection does not advance public-private partnerships.
- The Chamber believes that if DFS' cybersecurity regulations are correct and workable in practice (which DFS assumes) and covered entities can show that they are in compliance, then the covered entities should be legally protected.
- The amendment's notifications triggers are likely to be unworkable, leading to overreporting by covered entities. A middle-ground approach would feature the inclusion of a materiality threshold to appropriately calibrate the reporting of a cybersecurity event to the Department.
- DFS should consider modeling elements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The amendment needs to incorporate bilateral information-sharing provisions, such as providing covered entities with warnings, technical indicators, and related threat context.
- Absent substantial changes to its amendment, DFS should not move forward with finalizing its cybersecurity regulation.

If Correct, Then Protect: Government and Industry Need to Partner to Defend Covered Entities, Including Through the Establishment of Safe Harbor Provisions

The Department states in its APC that it declines to add safe harbor provisions to the amendment because the Department does not believe that they are necessary. The Department seems to suggest that covered entities mostly seek a safe harbor for situations involving noncompliance when the opposite is true, the Chamber believes.

The Chamber contends that when agencies regulate and covered entities can demonstrate compliance with the targeted program (e.g., DFS' cybersecurity regulation), then those covered entities should be protected from liability. Our members believe that simply having regulators pass judgment on the security posture of their business IT systems and operational technology is insufficient. In addition to the lack of liability protections, laws and regulations at the federal and state levels are not adequately helping defend the business community from criminal gangs and foreign powers.

DFS policy states, "The minimum requirements in Part 500 ensure that covered entities implement certain baseline cybersecurity protections or controls." (APC, p. 5) A fair corollary is that baseline policy should safeguard covered entities that can demonstrate their implementation of "certain baseline cybersecurity protections or controls." In many respects, it is the very least that policy can do owing to the fact that the business community is on the frontlines of protecting against and responding to an endless stream of cyberattacks.

Comment: **Several commenters requested that safe harbor provisions be added** [bolding added] with respect to various provisions of the amendment. . . .

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. (APC, pp. 7–8)

Commented [EMJ1]: The Chamber agrees with this thinking.

Commented [EMJ2]: The Chamber contends that a safe harbor is justified for covered entities that are compliant with DFS' cybersecurity regulation. Yet in its response, DFS seems to sidestep the issue of granting protections by focusing on noncompliance, a completely separate matter.

A legal safe harbor should apply to covered entities that implement and comply with DFS' cybersecurity regulation. Indeed, even DFS acknowledges that "entities should know whether they are in compliance," (APC, p. 83)—and thus should be able to voluntarily leverage a safe harbor, which the Chamber is calling for.

A reasonable corollary says that if DFS does not grant a safe harbor to compliant covered entities, then it is fair to call the soundness of the Department's cybersecurity regulation into question.

The Chamber is concerned that DFS' revised proposal continues to lack reasonable protections for covered entities. The Department and other government bodies are increasingly layering more cybersecurity regulations on financial services entities that are already burdened by nearly countless government mandates.

First, when covered entities demonstrate conformance with the cybersecurity regulation—including when they fulfill their reporting obligations—they should be expressly safeguarded. The amended cybersecurity regulation would require covered entities to certify compliance with all sections of Part 500. The Chamber contends that if covered entities demonstrate conformity with such certifications they should then receive express liability protections. Further, such legal protections should extend to nongovernment lawsuits generated by malicious cyber activity.

If DFS' cybersecurity regulations are correct and workable in practice, which the Department assumes, and covered entities can show that they are compliant, then the covered entities should be explicitly protected by law and regulation.

Second, it is reasonable that DFS should authorize safe harbors for covered entities when they meet the requirements of the cybersecurity regulation. The Chamber is not requesting the equivalent of a public policy free lunch—including for either the private sector *or* the public sector. Without a doubt, businesses bear the significant costs associated with nefarious cyber activity led by criminal organizations and nation-states.

The U.S. government monopolizes the authority to disrupt or halt malicious cyber activity at its source. Still, businesses in general, and cybersecurity-sophisticated companies in particular, regularly tell the Chamber that they cannot look to the federal government, much less to the states, to dismantle threat actors.

Third, businesses frequently tell the Chamber that it is in the interest of agencies—and not just industry—for them to do more than critique and regulate businesses' cybersecurity risk management programs. Both DFS and other government entities need to find creative ways to both share information with the private sector. Moreover, according to the White House's March 2023 *National Cybersecurity Strategy*, government needs to hold countries and criminals accountable for irresponsible behavior in cyberspace. Such activity would feature disrupting the networks of criminals behind dangerous cyberattacks in the U.S. and around the globe.[3] The business community needs both the federal government and DFS to step up their defensive partnerships in line with the cybersecurity substantial costs shouldered by covered entities.

The Amendment's Notifications Triggers Would Generate Needless Reporting by Covered Entities: The Inclusion of a Materiality Threshold Offers Government and Business a More Productive Approach

A continuing concern is the amendment's notification triggers, which need to be revised, including through incorporating a materiality threshold. As crafted, the amendment sets the notification bar so low that a flood of notifications to DFS would dilute the utility of reporting and essentially waste the time and resources of the business community.

Subsections (ii) and (iv) of section 500.17 prudently contain materiality thresholds related to the notification of cybersecurity events, but subsection (iii), in particular, does not. This arrangement would result in overreporting to DFS and potentially make covered entities liable for incidents that they are unaware of, given that a covered entity must report cybersecurity events that occur at the covered entity, its affiliates, or a third party service provider (TPSP). Accordingly, covered entities would likely be reporting on cybersecurity events (i) with little to no harm or significance in general and/or (ii) at an affiliate or a TPSP, even if there is practically no impact on these entities or on the covered entity itself.

[3] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Going further, without the inclusion of a materiality threshold, covered entities could be accountable for reporting on events at affiliates or TPSPs that they are unaware of. A company asked the Chamber, "If there is no impact and affiliates/third parties don't notify the covered entity, how would the covered entity be able to tell DFS?"

Therefore, the Chamber recommends revising the amendment in subsection (iii) to state, "(iii) cybersecurity events where an unauthorized user has gained access to a privileged account that materially harms the covered entity; or." The rationale here is that nearly any cybersecurity event where there is an unauthorized access to a privileged account would need to be reported to DFS. This would include incidents where there is no reasonable likelihood of material harm nor any impact on the covered entity's material information system or operations. The inclusion of a materiality threshold offers both DFS and covered entities a productive approach to fine-tuning notifications on cybersecurity events that really matter.

June 2023 revised proposed second amendment (p. 15)

Section 500.17 is amended to read as follows:

(a) Notice of cybersecurity event.

(1) Each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred at the covered entity, its affiliates, or a third party service provider that is [either] any of the following:

[(1)] (i) cybersecurity events impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; [or]

[(2)] (ii) cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity;

(iii) cybersecurity events where an unauthorized user has gained access to a privileged account that materially harms the covered entity; or

(iv) cybersecurity events that resulted in the deployment of ransomware within a material part of the covered entity's information system.

(2) Each covered entity shall promptly provide any information requested regarding such event. Covered entities shall have a continuing obligation to update and supplement the information provided.

***

Commented [EMJ3]: It is unclear when a covered entity's obligation to update DFS ends. A company told the Chamber that there should be a reasonable threshold upon which a covered entity no longer has to notify DFS.

November 2022 proposed second amendment (p. 15)

Section 500.17 is amended to read as follows:

(a) Notice of cybersecurity event.

(1) Each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred that is [either] any of the following:

[(1)] (i) cybersecurity events impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; [or]

[(2)] (ii) cybersecurity events that have a reasonable likelihood of materially harming, disrupting or degrading any material part of the normal operation(s) of the covered entity;

(iii) cybersecurity events where an unauthorized user has gained access to a privileged account; or

(iv) cybersecurity events that resulted in the deployment of ransomware within a material part of the covered entity's information system.

(2) Within 90 days of the notice of the cybersecurity event, each covered entity shall provide the superintendent electronically in the form set forth on the department's website any information requested regarding the investigation of the cybersecurity event. Covered entities shall have a continuing obligation to update and supplement the information provided.

(3) Each covered entity that is affected by a cybersecurity event at a third party service provider shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours from the time the covered entity becomes aware of such cybersecurity event.

DFS Should Model Elements of CIRCIA: The Amendment Needs to Incorporate Bilateral Information

As federal and state agencies increase their cybersecurity regulations on private entities, our nation's collective security and resilience will only improve if agencies elevate their roles and responsibilities too—particularly by providing businesses with novel warnings, technical indicators, and related threat context that are not commercially available.

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. (APC, pp. 8–9)

Commented [EMJ4]: The Chamber disagrees with DFS' response that "these [collaborative] initiatives would not affect the changes proposed in the amendment." Bilateral information sharing must be a core feature of DFS' amendment before it is finalized.

The Chamber includes both narrative text and a reference to CIRCIA in this letter, which we urge DFS to use in updating its cybersecurity regulation.

It is constructive that the Department is "exploring several initiatives to better support covered entities." Nonetheless, the amendment has a long way to go in bridging the gap between a regulation that is currently nonprotective and prescriptive and one that is protective and flexible. The Department outlines at length the statutory authority it has to establish new requirements, but the amendment does not say how the Department and other state officials would assist banking and financial services companies in ways that are truly collaborative and beneficial in defending against malign foreign cyber operations. This is a notable shortcoming of DFS' proposal, which the Chamber urges authorities to address.

In passing CIRCIA, Congress stated that the law should ensure bilateral information sharing between government and industry. According to CIRCIA, the Cybersecurity and Infrastructure Security Agency (CISA) would be required to—

- "Receive, aggregate, analyze, and secure" covered cyber incident reports to assess the "effectiveness of security controls, identify tactics, techniques, and procedures" that adversaries use to overcome the security controls.
- Coordinate and share information with federal agencies to "identify and track ransom payments," including ones utilizing virtual currencies.
- Leverage information gathered about cyber incidents to—
    - "[E]nhance the quality and effectiveness" of information sharing with appropriate entities (e.g., sector coordinating councils, technology providers, critical infrastructure owners and operators, and cyber incident response firms).
    - Provide appropriate entities with "timely, actionable, and anonymized reports of cyber incident campaigns and trends, including … related contextual information, cyber threat indicators, and defensive measures."
- Establish ways to receive feedback from stakeholders on how CISA can better receive reports and "most effectively support private sector cybersecurity."

- Facilitate the voluntary sharing of information between key critical infrastructure owners and operators regarding ongoing cyber threats or security vulnerabilities.

- Conduct a review of a "significant cyber incident," which includes a covered cyber incident/a ransomware attack, to identify and disseminate ways to prevent or mitigate similar incidents in the future.

- Review reports ("immediately") involving an ongoing cyber threat or security vulnerability for cyber threat indicators and defensive measures that can be anonymized and disseminated to appropriate stakeholders.

- Publish unclassified, public reports on a quarterly basis that describe "aggregated, anonymized observations, findings, and recommendations" based on covered cyber incident reports.

- Identify opportunities to "leverage and utilize data" on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and industry organizations.

- Make report information available to SRMAs and other appropriate federal agencies "as soon as possible but not later than 24 hours after the receipt of reports."[4]

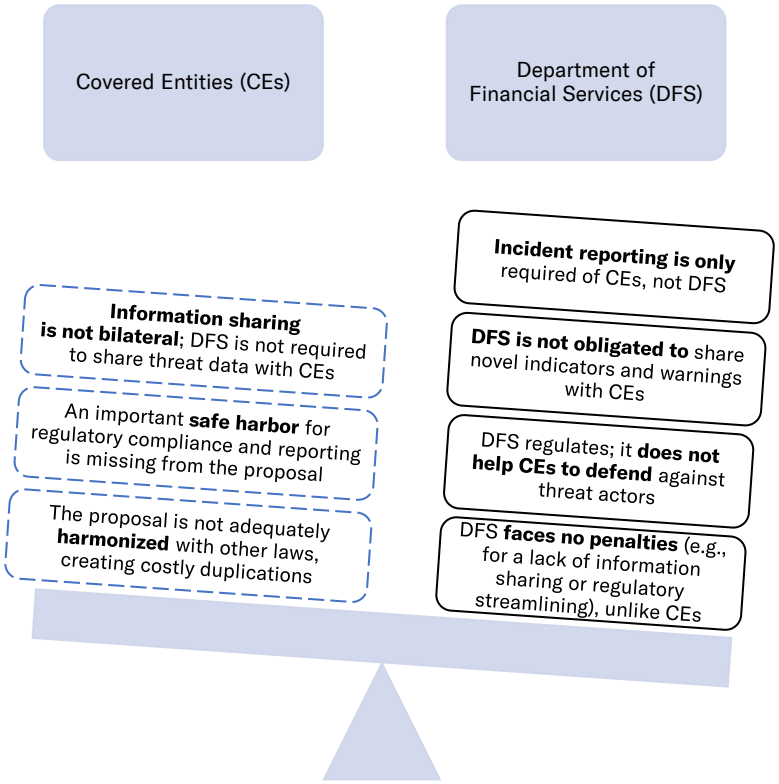
***

In sum, absent substantial changes to its proposal, DFS should not move forward with its amendment to its cybersecurity regulation. In the remainder of this letter, the Chamber annotates parts of our January 2023 letter to DFS based on selected excerpts from the APC (the text is shaded green). The Chamber does not address every aspect of the Department's June 2023 proposal. DFS should generally focus on the Chamber's comments on the right-hand side of the following pages.

[4] See section 2241 of CIRCIA (6 USC 681a), which is contained in division Y of the Consolidated Appropriations Act, 2022 (P.L. 117-103).
https://www.congress.gov/bill/117th-congress/house-bill/2471

Appendix A

Cybersecurity Policymaking Should Be Balanced for Optimal Outcomes, Not Tilted in Favor of Agency Interests (Selected Examples)



Would you agree to a law or regulation that is unbalanced or does not meet your cybersecurity interests?

- DFS is urged to remedy the imbalance in stakeholder interests before finalizing its cybersecurity regulation. Balanced policy is usually sustainable policy.
- Covered entities—including financial services firms with mature cybersecurity programs—receive limited support or actionable information from the federal government, much less from the states, to contest foreign malicious cyber activity. Notable exceptions include law enforcement.
- DFS' proposal should be reframed so that when covered entities meet the requirements of the cybersecurity regulation (e.g., to protect consumers and defend the stability of the U.S. financial system) they are granted a safe harbor.

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 9, 2023

Via cyberamendment@dfs.ny.gov

Joanne Berman
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: New York State Department of Financial Services; November 9, 2022, Proposed Second Amendment to Regulation 23 NYCRR 500 (DFS Cybersecurity Regulation)

Dear Ms. Berman:

The U.S. Chamber of Commerce appreciates the opportunity to comment on the New York Department of Financial Services' (DFS' or the Department's) second amendment to 23 NYCRR 500 (the amendment or the proposal), which governs cybersecurity requirements for financial services companies.[5]

The Chamber has been promoting sound cyber risk management practices domestically and overseas for more than a decade. Despite high-profile cyberattacks against public and private entities, we have seen a surge of business and government investments and innovations in the field of cybersecurity. Companies, not government, are the main force driving the protection and resilience of U.S. networks and information systems. In our experience, companies are increasingly integrating cybersecurity risk management practices into their corporate cultures. The Chamber wants to see this trend continue. We also want companies and agencies to work together in cyber risk management.

While the Chamber respects the efforts of DFS to amend Part 500, the Department should not move forward with its proposal unless substantial changes are made. The Chamber urges DFS to work directly with stakeholders to fashion a regulation that seriously takes other cybersecurity programs and rules into account, protects covered entities, and is workable in practice. Generally, covered entities take a best-practice, risk-based approach to their cybersecurity programs and policies to make their information systems resilient and to safeguard personal data.

[5] https://www.dfs.ny.gov/industry_guidance/cybersecurity
https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf

I. The Chamber Supports Strong, Protective Cybersecurity Programs.

The Chamber believes that protecting key critical infrastructure (e.g., assets, systems, and data of financial institutions) from malign cyber activity is a top economic and national security priority. For several years, federal, state, and local governments and industry have embraced a partnership model to defend critical infrastructure—the majority of which is owned and operated by the private sector—from nation-state and criminal hacking campaigns. This approach has been largely successful. Many focus on the unfortunate cyber incidents that occur, while too few focus on the countless cyber incidents that have been avoided.

The Chamber has serious, ongoing concerns with the proliferation of cybersecurity laws, regulations, and guidance documents at the state, federal, and international levels. Although it is a significant actor, DFS is just one of many governmental bodies that are promulgating broad and detailed cybersecurity regulations impacting industry and financial services companies in particular.

Despite industry's urgings, governmental authorities are making insufficient progress in harmonizing[6] the multiple cybersecurity rules that businesses must comply with—and the list continues to increase.[7] Due to the pronounced lack of harmonization, businesses face a number of challenges.

---

[6] In 2016, the Chamber wrote to DFS on its proposed cybersecurity requirements for financial services companies. The state of harmonization since then remains largely unchanged.

Among other things, the letter stated, "[The Chamber] urge[s] policymakers at all levels of government to help agencies and departments *harmonize* existing regulations with the [Cybersecurity] Framework. … A single business organization should not be beset by multiple cybersecurity rules coming from many agencies, which are likely to be conflicting or duplicative in execution." The letter added that "DFS is moving fairly swiftly on a top-down, complicated rulemaking that would benefit from lengthier, in-depth scrutiny."
https://www.uschamber.com/assets/documents/nysdfs_leter_on_cyber_requirements_final.pdf

[7] During a National Institute of Standards and Technology (NIST) workshop on updating the Cybersecurity Framework, a financial services professional noted that her company operates in 60 countries, is regulated by 140 bodies, and is governed by 2,300 regulations. She said that the resulting global proliferation of cybersecurity laws, regulations, guidance, and frameworks has "created an immense drain" on internal resources. She added that an industry survey conducted in 2016 found that 40% of the CISO's team's time is spent on compliance.

NIST, "Journey to the NIST Cybersecurity Framework (CSF) 2.0, Workshop #1, Panel 2: Lessons Learned from Development and Use of CSF Profiles," August 17, 2022.
https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1

Key Points

- The Chamber respects the efforts of DFS to amend Part 500, but the Department should not move forward with its proposal unless substantial changes are made. The Chamber urges DFS to work with stakeholders to develop a flexible regulation that takes other cybersecurity programs and rules into account, protects covered entities, and is workable in practice.
- The amendment is not harmonized with other state, federal, and international requirements. It clearly establishes duplicative and/or conflicting requirements (e.g., cybersecurity event notification) that come with imprudent trade-offs.
- The amendment would cover too many entities in contrast with basic risk management principles. Many financial services companies already spend a disproportionate amount of time and resources complying with governmental cybersecurity laws, regulations, and guidance documents at home and internationally. Compliance does not equate to enhanced security.
- Industry investments in cybersecurity are expensive, and they must be made and used wisely. Public policy needs to enhance businesses' cybersecurity, but the amendment could do the opposite.
- The Department's proposal does not contemplate helping covered entities defend themselves against criminal organizations (e.g., ransomware attacks) and malicious foreign actors. DFS should include more flexible and collaborative approaches to security and resilience.
- The amendment would micromanage covered entities' cybersecurity programs and their boards. The Department has neither adequately explained how its proposal would protect the public nor justified its costs against the purported benefits.
- It is striking to the Chamber that the amendment does not seek to safeguard covered entities for their conformity to strong standards (e.g., authorizing legal liability protections) but rather penalize them for even relatively brief lapses in compliance.
- The Chamber strongly opposes prescribe-and-penalize approaches to cybersecurity policymaking, especially when agencies neither protect businesses nor take proactive actions to disrupt or degrade the operations of illicit cyber actors.

First, a significant number of businesses contend that their criticisms of cybersecurity policies and regulations—which are based on professionals' practical experiences and technical expertise—are often dismissed by regulators. Further, many businesses believe that they need to accommodate regulators without voicing such concerns because of the authority that officials wield. Such thinking, which the DFS amendment embodies, does not yield positive cybersecurity outcomes.

What is chiefly troublesome to the Chamber, the amendment would create new and overlapping requirements in relation to existing laws—cyber event notifications being a prime

example—and grant DFS new powers that may not improve the cybersecurity of covered entities, New York State, and our country. The Department's amendment would spur penalties against covered entities for even temporary lapses in compliance. To illustrate, DFS' proposal would require covered entities to stipulate in writing whether they are compliant with Part 500 (section 500.17). Entities that are not in compliance with any section of Part 500—even for a period of 24 hours—could be subject to DFS sanction (section 500.2).

Second, government authorities frequently use cyber incidents at a victim company to justify casting a wide regulatory net over multiple entities—many of which may already manage cybersecurity programs that are strong and adaptive in the face of evolving cyber risks and threats. Regulators should focus their activities on working with covered entities where they have fallen short meeting the terms of Part 500, not expanding their authority, such as covering class A companies (section 500.1(c)). DFS' amendment contains new prescriptions that may not fit with covered entities' existing cybersecurity policies and programs or make sense for each company to implement.

Third, the Department's proposal lacks safeguards for covered entities that demonstrate conformity with industry-led, globally accepted cybersecurity standards. Cyber programs that the Chamber generally supports grant clear protections to regulated entities. The amendment should be revised to authorize clear protections for compliant entities. (See Appendix [B].)

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.

Commented [EMJ5]: The Chamber strongly contends that the amendment to the Department's cybersecurity regulation should not be completed without a safe harbor. Prescription without protection is unnecessary and would not advance public-private security partnerships.

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. (APC, pp. 7–8)

Fourth, the amendment needs to foster a more cooperative, less adversarial relationship between industry and DFS. To begin with, financial services entities with mature cybersecurity programs receive comparatively limited support or actionable information from the federal government, much less from the states, to contest foreign malicious cyber activity. Notable exceptions include law enforcement.

DFS outlines at length the statutory authority it has to set forth new requirements, but the amendment does not say how the Department and other state officials would assist financial services companies in ways that are truly collaborative and beneficial (e.g., providing novel threat indicators and warnings) in defending against malign foreign cyber operations. This is a notable shortcoming of DFS' proposal, which the Chamber urges authorities to address.

Fifth, DFS believes it is ensuring that all financial services providers regulated by the Department have cybersecurity programs that meet minimum cybersecurity standards to protect consumers, operate safely, and defend the stability of the U.S. financial system.[8]

The Chamber opposes cybersecurity nonprotective policies that are overly broad, top-down in nature, and not streamlined with other governmental rules because the inevitable result is duplicative and/or conflicting requirements. As such, DFS' amendment is likely to divert valuable cybersecurity resources away from covered entities' enterprise risk management programs to meet the regulatory mandates. Moreover, the amendment would add to pronounced inefficiencies, notably in the area of cyber incident reporting.

In sum, absent substantial changes to its proposal, DFS should not move forward with its amendment to Part 500.

II. Critique of the Amendment: Prescriptive, Redundant, and Conflicting Requirements Detract From Security and Resilience.

A company told the Chamber that prescriptive cybersecurity requirements reinforce a "compliance mindset." Under rules like Part 500, covered entities are pushed to adopt

[8] Regulatory Impact Statement for the Proposed Second Amendment to 23 NYCRR Part 500 (SAPA), p. 3.
https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_sapa_20221109.pdf

arbitrarily identified security controls that can create a false sense of security. Some organizations' leaders believe that they have met their obligations by implementing the compliance requirements. Some members of the public feel that their service providers are doing everything they can to protect their data. Instilling a compliance mindset can do a disservice to the individuals that DFS is trying to protect.

Moreover, prescriptive requirements are often ill-tailored and lose effectiveness as new technologies are developed, security risks change, and consumer behaviors evolve. Alternatively, an approach to information security that places the onus on the covered entity to continually manage its security risks and resilience is the optimal route to take.

The Chamber's feedback does not cover every aspect of the proposed amendment to the cybersecurity regulation. It focuses on important themes, definitions, and related provisions.

A. Main Themes

1. **The amendment's scope should be narrowed. It needs to focus on enabling risk management and helping defend covered entities.**

1.1. DFS' proposal to amend Part 500 would enlarge its reach into the business community, as well as the networks and information systems of currently regulated parties. The Chamber recommends against taking such an aggressive step.

- Instead of expanding the scope of covered entities, DFS should expressly limit the scope of the regulations to data and information systems (section 500.1(g)) that support regulated activities in which DFS has explicit regulatory authority.

- A sizeable number of nonfinancial services firms that are potentially subject to DFS jurisdiction could have numerous information systems that support business operations and networks that do not fall within DFS' traditional purview.

- DFS should expressly limit the scope of its regulations to data and information systems that support regulated activities in which the Department has a clear regulatory interest.

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. (APC, pp. 9–10)

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. (APC, pp. 12–13)

Commented [EMJ6]: A company told the Chamber that the amendment's scope should be narrowed. "It needs to focus on enabling risk management and helping defend covered entities." The company added, "If the Department proceeds with such a broad interpretation of the regulation's scope, companies may cease offering services to the detriment of New York State residents."

The Chamber believes that if DFS expands the scope of its cybersecurity regulation, it should also expand the scope of its public-private collaboration, such as sharing of threat data with covered entities. In a nutshell, a balanced approach to public policy means that if DFS is unable to increase collaboration with covered entities, it should not increase the regulation of covered entities.

1.2. The proposed amendment's broadened scope would subject covered entities to redundant governmental cybersecurity regimes.

- Regulatory overlap does not equate to an increase in entities' security and resilience. Instead, it typically leads to costly duplication and inconsistent requirements among multiple regulations.
- Such outcomes create powerful inefficiencies for regulated entities. They undercut existing cybersecurity programs because of competition among regulators for the limited cybersecurity resources of covered entities.
- By eschewing a focused approach to cybersecurity oriented toward risk, the amendment would undermine DFS' security goals, specifically among sophisticated industry organizations. The amendment would substitute the judgment of industry leaders, technical experts, and information security professionals in assessing and managing threats and vulnerabilities.[9]

[9] Raymond J. Decker, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T, U.S. Government Accountability Office, October 12, 2001.

- DFS should not presume to make criticality assessments (i.e., what is important) for covered entities. The Department lacks the information that covered entities have to make such calls. Firms must improvise and dedicate resources in real time to combat myriad cyber threats.

1.3. As of this writing, DFS has not proposed establishing a protective program for current or potentially covered entities.

- The definition of a covered entity should not be revised to include class A companies, which section 500.1(c) proposes.

- The grouping of covered entities should be risk based and limited to private entities that DFS is both able and willing to assist at the request of the covered entity before, during, and/or after a significant cyber incident.

- DFS' regulation should articulate what level of assistance it could extend to covered entities. Something is amiss in policymaking circles when an expansive regulatory push is married to little, if any, assistance to covered entities.

- If the Department is unable to render assistance (e.g., providing novel cyber threat indicators and warnings to covered entities today), it should not expand the scope of Part 500. It is fair to say that DFS, like any government agency, must be able to support the defense of industry, not just prescribe requirements and pass judgment on the security postures of regulated parties.[10]

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. (APC, pp. 8–9)

Commented [EMJ7]: DFS' response is constructive, but the Department needs to do much more. See the Chamber's recommendations tied to CIRCIA.

https://www.gao.gov/products/gao-02-150t

[10] For more on Chamber thinking about how policymakers should assist critical infrastructure entities in ways that are collaborative and beneficial in defending against malign foreign cyber operations, see our September 16, 2022, letter on systemically important entities legislation. https://www.uschamber.com/assets/documents/220916_Coalition_SIEAmendmentH.R.7900NDAA_SASC-HSGAC.pdf

1.4. Cyber incident reporting, which the Department calls for, must not be an end in itself.

- The Chamber generally supports workable policy that leads to industry groups receiving actionable threat data and assistance from government agencies, including DFS.

- The Chamber is uncertain about what DFS plans to do with the data it collects, save for possibly sanctioning covered entities. To our knowledge, the amendment puts forward no plans for fostering bilateral information sharing between the Department and covered entities.

- The amendment needs revising to require deeper information sharing with covered entities. A business principal told the Chamber, "The amendment mandates the reporting of a 'cybersecurity event' to DFS but lacks reciprocal data sharing. This is not beneficial to security. It is not a public-private partnership."

2. The amendment lacks harmonization with similar requirements. To be workable, cyber incident reporting should align with CIRCIA.

2.1. DFS' amendment would include changes to section 500.17 pertaining to notifying the Department about certain cybersecurity events. The Chamber urges DFS to revise its proposal so that Part 500 aligns with global and leading federal reporting policies and processes.

2.1.1. The Chamber has undertaken extensive work in this space. In December 2022, the Chamber released a policy brief urging governments around the world to harmonize various cyber incident reporting regimes. The paper advocates for a thoughtful set of policy recommendations for consideration by public authorities when they take legislative or regulatory actions.[11]

2.1.2. A logical place to start is the bipartisan CIRCIA, which passed in March 2022 with support from the business community. The Chamber worked closely with the U.S. Congress between 2021 and 2022 to develop and pass CIRCIA and submitted comments in November 2022 in response to CISA's request for information on implementing the law.[12]

---

[11] U.S. Chamber of Commerce, *Global Cybersecurity Incident Communications: Notification, Reporting, and Information Sharing Policy Brief*, December 14, 2022. https://www.uschamber.com/assets/documents/FINAL-Issue-Brief-Global-Cyber-Incident-Reporting.pdf

Sara Friedman, "U.S. Chamber offers recommendations for global policymakers on cyber incident reporting," *Inside Cybersecurity*, December 15, 2022. https://insidecybersecurity.com/share/14179

[12] Sara Friedman, "U.S. Chamber encourages CISA to seek 'qualitative' information in [supplemental] incident reports under upcoming mandatory regime," *Inside Cybersecurity*, November 30, 2022.

- **Tailor the number of covered entities.** The Chamber believes that the proposed scope of covered entities in DFS' proposal would be exceedingly broad from a risk management perspective. Indeed, the amendment would heighten DFS' challenge by adding a new category of covered entities (i.e., class A companies) under section 500.1(c).

  For Part 500 to be effective, the Department should establish criteria in the amendment that creates a targeted list of covered entities that if impacted could create significant consequences within covered entities, New York State, and the U.S.

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. (APC, p. 12)

- **Target reporting to a significant, confirmable cyber incident.** DFS should focus on the types of significant cyber incidents that it wants covered entities to report. In other words, consideration should be given to placing emphasis on addressing a confirmable, significant cyber incident in order to mitigate its impact rather than on entities.

- The Chamber holds that cybersecurity reporting should be geared toward significant and relevant incidents—the point being that the bar should be set high for the types of incidents that DFS would determine to be reportable.

- The amendment should link reporting to confirmed cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and verified cyber incidents.

---

https://insidecybersecurity.com/daily-news/us-chamber-encourages-cisa-seek-%E2%80%98qualitative%E2%80%99-information-incident-reports-under-upcoming

- Policy, legislative, and regulatory language that the Chamber has considered (e.g., potential cyber intrusions) would likely be unworkable in practice. Comparatively loose definitions would yield extraneous information that does not improve the situational awareness of DFS and other covered entities.

  For example, the vague language in the proposed section 500.1(e), "any act or attempt, successful or unsuccessful" to gain unauthorized access to disrupt or misuse an information system, would lead to an overabundance of reporting to DFS.

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 § t § 500.17(a). (APC, pp. 13)

Commented [EMJ8]: The Chamber believes that DFS' call for reporting on "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system" is misguided.

First, DFS should link reporting to confirmed cybersecurity incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed cybersecurity incidents. Some legislative language that we have considered—such as "potential cyber intrusions" and incidents that could be "reasonably believed" to be reportable—is overly subjective. The definition of a "cybersecurity event" should be attached to clear, objective criteria in DFS' cybersecurity regulation.

Second, the bar for the types of cybersecurity events that DFS would determine to be reportable is much too low. Reporting the vast number of events of comparatively little importance could easily overwhelm DFS.

Third, covered entities should not be forced to report insignificant (e.g., unsuccessful) cyber activity when reports on harmful incidents are needed most by stakeholders.

- DFS should adopt the position that only reports that go to CISA under CIRCIA should be noticeable to the Department under an amended Part 500.

- **Maintain the 72-hour reporting deadline.** It is constructive that the amendment features a notification timeline of "… in no event later than 72 hours from a determination that a cybersecurity event has occurred." This phrasing tracks with a 72-hour deadline under CIRCIA.

The Department's Proposed Definition and Notice Regarding a 'Cybersecurity Event'

As written, the amendment would lead to overreporting

Section 500.1 [(d)] (e) *Cybersecurity event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.

Comment: Several commenters suggested that § 500.17(a)(1)(iii) is too broad and would result in overreporting 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. (APC, p. 80)

Commented [EMJ9]: The Chamber welcomes this expected revision to the Department's proposal.

Consistency of Definitions

A 'cybersecurity event' should be changed to a 'cyber incident'; a cyber incident is also significant and confirmable and starts the 72-hour reporting clock

- In writing CIRCIA, the U.S. Congress was clear that the definition of a cyber incident should be set at a level to not flood the government with unnecessary reporting. In other words, comparatively routine occurrences of malicious cyber activity should not be reported.

- The Chamber believes that a rational definition of "incident" in the cybersecurity context is found in 6 U.S. Code § 659, which defines an incident as an "occurrence"—not merely a hypothetical or an unsuccessful event—and such an occurrence must "actually or imminently" cause one of the enumerated jeopardies to data or information systems without lawful authority.[13]

- To avoid confusion and inconsistent interpretations by policymakers and stakeholders, the term "cybersecurity event" should be changed to "cyber incident" to address the same areas of concern as a "significant cyber incident" as found in Presidential Policy Directive 41 (PPD 41). Namely, a covered cyber incident would result in "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[14]

[13] 6 U.S. Code § 659(a)(5) ("[T]he term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system").
https://www.law.cornell.edu/uscode/text/6/659

[14] PPD 41, *United States Cyber Incident Coordination*, July 26, 2016.

- The 72-hour notification clock should begin when a covered entity has forensically completed an initial assessment of a covered cyber incident.

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) [see here].

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

Commented [EMJ10]: Cybersecurity information sharing needs to be bidirectional and safeguarded, consistent with CIRCIA and the Cybersecurity Information Sharing Act of 2015. For example, under CIRCIA, both covered and voluntarily reporting entities and their information are safeguarded. In addition to legal liability protections, CIRCIA contains provisions that would—

• Prohibit federal and state governments from using submitted data to regulate reporting entities.
• Treat reported information as commercial, financial, and proprietary.
• Exempt reported information from federal and state disclosure laws.
• Preserve trade secret protections and any related privileges or protections.
• Waive governmental rules related to *ex parte* communications.

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

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. (APC, pp. 4–6)

2.2. The proposed notification triggers should be reconsidered, including incorporating key materiality thresholds. As crafted, the amendment sets the notification bar so low that a flood of notifications would dilute the utility of reporting.

Proposed Notifications Triggers

Provisions would lead to extraneous reporting; they should be deleted or revised

(iii) material cybersecurity events where an unauthorized user has gained access to a privileged account; or [section 500.17(a)(1)(iii)]

Chamber recommendation: A notification for unauthorized access to a privileged account should only apply where such account had access to nonpublic information or where such access was for a prolonged period of time.

(iv) material cybersecurity events that resulted in the deployment of ransomware within a **material** [emphasis added] part of the covered entity's information system. [section 500.17(a)(1)(iv)]

Chamber recommendation: A notification for a ransomware incident should only apply where the deployment of ransomware has a material impact on a material part of the covered entity's information system.

(3) Each covered entity that is materially harmed ~~affected~~ by a cybersecurity event at a third party service provider shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours from the time the covered entity becomes aware of such cybersecurity event. [section 500.17(a)(1)(3)]

Chamber recommendation: For purposes of this clause, materiality is in reference to the covered entity, not the third party service provider. An event that is material to the third party service provider but that does not cause material harm to the covered entity should not require notification to DFS.

- To enhance reporting efficiency and useful outcomes for DFS and industry, the Department's definition of a cybersecurity event should be revised. Notices should

Commented [EMJ11]: The amendment falls short of the regulatory alignment or harmonization needed to foster the cybersecurity postures at covered entities that both businesses and DFS seek. It also overlooks the White House's thoughtful push to harmonize and streamline new and existing regulations, including enabling regulated entities to afford quality security. https://www.whitehouse.gov/oncd/briefing-room/2023/07/19/fact-sheet-office-of-the-national-cyber-director-requests-public-comment-on-harmonizing-cybersecurity-regulations

Many companies tell the Chamber that the meaningful lack of alignment is generally zero-sum. That is, cybersecurity professionals are increasingly made to shift their roles toward compliance and away from defense. Such a situation is in neither DFS' nor covered entities' interests.

In addition, DFS is urged to take these three publications into account as it makes decisions regarding regulatory alignment.

• The Financial Stability Board's *Enhancing Third-Party Risk Management and Oversight* toolkit (June 22, 2023). https://www.fsb.org/2023/06/enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities-consultative-document

• Financial Stability Institute's *Banks' Cyber Security—A Second Generation of Regulatory Approaches* paper (June 12, 2023). https://www.bis.org/fsi/publ/insights50.htm

• Federal bank regulatory agencies final guidance on third-party risk management (June 6, 2023). https://www.federalreserve.gov/newsevents/pressreleases/bcreg20230606a.htm

be triggered only when there is a reasonable likelihood of a significant cyber incident or harm to the economic security of New York State and U.S. national security akin to PPD 41.

- The amendment appears to incorporate a constructive materiality threshold related to a ransomware deployment under section 500.17(a)(1)(iv). Yet it lacks a similar standard regarding the ransomware event itself, as well as unauthorized access to a privileged account or a cybersecurity event at a third party service provider (section 500.17(a)(1)(3)). The triggering events lack an element of harm or tangible maliciousness.

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 overreporting 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. (APC, p. 80)

- Without additional refinements, these three notification requirements would impose unhelpful reporting requirements on covered entities. The results would include an over-notification to DFS by covered entities with little to no benefit to the Department, consumers, or the financial services community.

- The Chamber urges DFS to consider whether these additions are necessary given the substantial overlap between them and existing notification requirements. After all, an event would be reportable to DFS where a third party service provider or unauthorized access to a privileged account has the likelihood of materially "harming, disrupting or degrading any material part of the normal operation(s)" of the covered entity, or would otherwise result in a notification to another government body.

- The Chamber believes that cybersecurity reporting should be geared toward significant and relevant incidents—the point being that the bar should be set high for the types of incidents that DFS would determine to be reportable. Neither covered entities nor the Department would benefit from an abundance of cyber "noise."

2.3. The amendment falls well short of protected, bilateral information sharing. In addition, the amendment does not appear to address what DFS would do with reported information to provide indicators and warnings to covered entities and other industry stakeholders.

- DFS needs to treat notifications as a means to bidirectional sharing and collaboration, including helping law enforcement identify and prosecute bad actors.

- Cybersecurity notices need to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation and/or prevention of future cyber incidents.

- Cybersecurity information sharing needs to be bidirectional and safeguarded, consistent with the Cybersecurity Information Sharing Act of 2015.[15] For example, under CIRCIA, both covered and voluntarily reporting entities and their information are safeguarded. In addition to legal liability protections, CIRCIA contains provisions that would—

    - Prohibit federal and state governments from using submitted data to regulate reporting entities.
    - Treat reported information as commercial, financial, and proprietary.
    - Exempt reported information from federal and state disclosure laws.
    - Preserve trade secret protections and any related privileges or protections.
    - Waive governmental rules related to *ex parte* communications.[16]

[15] CISA 2015 (see title N of P.L. 114-113), which had the support of both parties in Congress and the Obama administration, is a good example of a program that encourages businesses to defend their computer systems and share cyber threat data with government and private entities within a protective policy and legal structure.
https://www.congress.gov/bill/114th-congress/house-bill/2029
https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance

[16] https://www.uschamber.com/assets/documents/221114-CIRCIA-RFI_USCC-Comments_Final.pdf

- Any generally valid regulation that DFS or another governmental body promulgates should protect covered entities in ways virtually identical to CISA 2015, among other laws and programs.[17]

Comment: One commenter . . . . also mentions the lack of protections similar to those found in 6 U.S.C. § 681e(b) [see here].

Response: . . . . 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. ... 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. (APC, pp. 4–6)

- The Chamber believes that DFS needs to take a much more assertive role in collaborating with businesses to proactively defend their data, devices, and systems. It should be increasingly regarded as unacceptable for any government agency to prescribe regulations, play a passive role in deterring/defending against malign actors, and yet pass judgment on industry victims.

3. Changes to Part 500 should not include micromanaging boards and CISOs.

3.1. DFS' proposal introduces a new definition of senior governing body to Part 500. It plays a role in pushing a covered entity's board of directors in a direction akin to day-to-day management.[18]

[17] The 2018 Ohio Data Protection Act (S.B. 220) is a notable model that the Chamber supports. Ohio enacted this innovative data security/cyber law in November 2018. S.B. 220 grants an affirmative defense against data breach tort claims to those businesses whose cybersecurity plans leverage an acceptable industry standard; other states' data protection laws focus on requirements or penalties. https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220 https://moritzlaw.osu.edu/data-and-governance/wp-content/uploads/sites/105/2019/03/cybersecurity-whitepaper-32819F-1.pdf

[18] See the Chamber's May 9, 2022, letter to the Securities and Exchange Commission (SEC) on the agency's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposal. https://www.sec.gov/comments/s7-09-22/s70922-20128398-291304.pdf

Section 500.1(p). *Senior governing body* means the covered entity's board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer of the covered entity responsible for the covered entity's cybersecurity program.

- According to section 500.3, each covered entity shall implement and maintain a written policy or policies—covering, minimally, a dozen-plus areas—that would be "approved at least annually" by the senior governing body. The proposal would make significant changes to how a covered entity governs its cybersecurity program and policies.

- The result is an unnecessary micromanagement of covered entities pertaining to the functioning of both the management and the boards of companies. The Department has neither adequately explained how its proposal would protect the public nor justified its costs against the purported benefits.

- Chamber members note that several of the policies DFS would mandate are on development, implementation/revision, and approval time frames that can take more than a year to complete and are not likely able to be artificially batched together for annual approval.

- The amendment should retain the ability of a senior officer to approve a covered entity's cybersecurity policies and require annual approvals when material changes to the policies have been made.

DFS amendment

Section 500.3 [Cybersecurity policy.] Each covered entity shall implement and maintain a written policy or policies, approved at least annually by [a senior officer or] the covered entity's [board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures] senior governing body for the protection of its information systems and nonpublic information stored on those information systems. ...

Chamber recommendation

[Cybersecurity policy.] Each covered entity shall implement and maintain a written policy or policies, with any material changes approved at least annually by ~~[~~a senior officer or~~]~~ the covered entity's [board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures] senior governing body for the protection of its information systems and nonpublic information stored on those information systems. ...

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.

Commented [EMJ12]: A covered entity's cybersecurity policy/program should be approved and implemented by management and reviewed by the board. The Chamber would point to the Gramm-Leach-Bliley Act (GLBA) as a key precedent. Under the GLBA, an entity's cybersecurity policy/program is approved once by the board and reviewed thereafter. DFS should align with this model.

While the board or an appropriate committee of the board is required to initially approve an entity's cybersecurity policy/program, the reporting obligation requires an entity to provide a report to the board or an appropriate committee of the board at least annually.

In essence, the report describes the overall status of the cybersecurity policy/program and the entity's compliance with the GLBA guidelines. The report may cover material matters related to the entity's cybersecurity policy/program. What's key is that the GLBA does not require an annual approval by an entity's board.

Commented [EMJ13]: Once an entity's cybersecurity policy/program is initially approved, the GLBA only requires an annual review by the board.

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. (APC, pp. 22–23)

Commented [EMJ14]: The Chamber is not solely focused on the regulation being overly burdensome. The issue is that the board should be conducting oversight, separate from management's approval and the implementation of a covered entity's cybersecurity policy/program.

- The proposed section 500.4(c) requirement is not appropriate for all boards of a covered entity. The recipients of "timely" reporting by a CISO should be a covered entity's senior managers. CISOs are called on to annually report to the senior governing body under the proposed changes to section 500.4(b).

- The Chamber believes that section 500.4(c) should be revised to require that only material cybersecurity issues need to be timely reported to the senior managing officer or the board.

DFS amendment

Section 500.4(c). (c) The CISO shall also timely report to the senior governing body regarding material cybersecurity issues, such as updates to the covered entity's risk assessment or major cybersecurity events.

Chamber recommendation

(c) The CISO shall also timely report to the senior officer or to the senior governing body regarding material cybersecurity issues, such as material updates to the covered entity's risk assessment or ~~major~~ material cybersecurity events.

- A number of industry organizations strongly question the need for including section 500.4(d) in Part 500. The Chamber believes that it should be removed from DFS' amendment.
- A covered entity is currently mandated under Part 500 to develop, implement, and maintain a cybersecurity program to protect its information systems. Section 500.4(d)(2) is unnecessary.
- The Chamber contends that DFS should not dictate how a covered entity organizes its board and how the board conducts risk management with senior company leadership. Under the amendment, DFS would essentially insert itself into how all covered entities would design their plans to detect, respond to, and recover from cyber incidents.

DFS amendment

Section 500.4(d). (d) If the covered entity has a board of directors or equivalent, the board or an appropriate committee thereof shall:

(1) exercise oversight of, and provide direction to management on, the covered entity's cybersecurity risk management;

(2) require the covered entity's executive management or its delegates to develop, implement and maintain the covered entity's cybersecurity program; and

(3) have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management.

Chamber recommendation

Section 500.4(d). (d) If the covered entity has a board of directors or equivalent, the board or an appropriate committee thereof shall:

(1) exercise oversight of~~, and provide direction to management on,~~ the covered entity's cybersecurity risk management;

(2) require the covered entity's executive management or its delegates to develop, implement and maintain the covered entity's cybersecurity program; and

(3) have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management.

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

Commented [EMJ15]: The requirement for a covered entity's CISO to have the "ability to direct sufficient resources to implement and maintain an effective cybersecurity program" is remarkably prescriptive. It contrasts with DFS' commentary that CISOs would not be given a so-called blank check.

DFS needs to explicitly state that the CISO is not the person who would be making a covered entity's cybersecurity resourcing decisions. A company told the Chamber, "It seems that DFS is trying to set up a framework for increased enforcement actions against covered entities."

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. (APC, pp. 27–29)

***

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. (APC, pp. 30–33)

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.

Commented [EMJ16]: The Chamber appreciates that DFS plans to make this deletion.

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. (APC, pp. 33–35

3.2. The Chamber disagrees with the requirement in section 500.4(d)(3) for boards to have "sufficient expertise and knowledge."

- Board experts should not proliferate via implicit or explicit government directives. From an industry standpoint, the Chamber does not think that DFS should dictate or suggest which experts sit on companies' senior governing bodies.

- Cybersecurity talent is scarce globally. From a personnel standpoint, it is unclear where covered entities would get the so-called cybersecurity expertise that the proposal would mandate.[19] There is a well-documented lack of cybersecurity talent for the public and private sectors that would unquestionably affect covered entities' recruitment of board cybersecurity experts.[20]

[19] For example, see (ISC)[2] blog, "Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022," February 15, 2017. By one estimate, the cyber workforce gap is estimated to be growing, with the projected shortage reaching 1.8 million professionals by 2022.
http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

House Homeland Security Committee Cybersecurity and Infrastructure Protection Subcommittee hearing, "Challenges of Recruiting and Retaining a Cybersecurity Workforce," September 7, 2017.
https://homeland.house.gov/hearing/challenges-recruiting-retaining-cybersecurity-workforce

[20] Quality information on this subject is available via CyberSeek, which has produced an interactive heat map with insights into the supply and demand for cybersecurity professionals in the U.S., including data on state and metropolitan areas. According to CyberSeek, there are approximately 598,000 cybersecurity job openings in the U.S. This significant number does not account for workforce shortfalls in other parts of the world.
https://www.cyberseek.org/heatmap.html

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. (APC, pp. 36–37)

Commented [EMJ17]: The Department's revision would be a positive development.

B. Definitions and Other Key Provisions

Multi-factor authentication or MFA (section 500.1[(f)] (h); section 500.12). A Chamber priority regarding this section is to ensure that the amendment does not deprecate the use of SMS text messages for MFA. We urge DFS to take an approach that enables covered institutions to make appropriate security decisions for their organizations and customers based on the sensitivity of the data that needs to be protected and the management of risk.

The amendment would seemingly eliminate text messaging on a mobile phone from Part 500. The Chamber interprets this change as not forbidding financial institutions from using SMS text messages as a possession factor for MFA. The language of the definition would seemingly neither prohibit nor recommend the use of SMS text messages.[21] The Chamber urges DFS to confirm that it is not prohibiting the use of SMS texting. There are instances where SMS texting may be appropriate, but the covered entity needs to make this determination based on an assessment of risks.

DFS amendment

[(f)] (h) *Multi-factor authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) knowledge factors, such as a password;

(2) possession factors, such as a token[or text message on a mobile phone]; or

(3) inherence factors, such as a biometric characteristic.

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.

[21] See, relatedly, the Federal Trade Commission (FTC) final rule, "Standards for Safeguarding Customer Information," *Federal Register*, December 9, 2021, p. 70277. https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information

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. (APC, p. 16)

Section 500.12 is amended to read as follows:

(a) Multi-factor authentication[. Based on its risk assessment, each covered entity] shall [use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems.] 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 section 500.19(a) of this Part, in which case multi-factor authentication shall be utilized for:

(1) remote access to the covered entity's information systems;

(2) remote access to third party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and

(3) all privileged accounts other than service accounts that prohibit interactive login.

(b) [Multi-factor authentication shall be utilized for any individual accessing the covered entity's internal networks from an external network, unless] If the covered [entity's] entity has a CISO, [has approved] the CISO may approve in writing the use of reasonably equivalent or more secure [access] compensating controls. Such controls shall be reviewed periodically, but at a minimum annually. (Revised proposed second amendment, p. 10)

Commented [EMJ18]: The proposed MFA requirements are overly prescriptive. Covered entities should be able to make decisions based on their own assessments of risk. However, the "any individual accessing" wording seems to undercut risk-based judgments.

For example, would "any" access include physical access? If an employee enters a covered entity's building using an access card, would this count as part of the MFA process? In short, the use of "any" encompasses numerous methods of access that would fail to appropriately account for the inevitable acceptance of some risk.

Also, a company said that for covered entities without a presence in New York State, the MFA requirements could exceed DFS' jurisdiction. "For example, would this mandate compel MFA for consumers in other states to log in to an online portal?" The company added, "The result could be a state-by-state approach to regulating MFA, including being in conflict with the Federal Trade Commission's Safeguards Rule, which would be highly burdensome and inefficient."

Privileged account (section 500.1(l)). A privileged account is generally understood to be an account that provides privileges beyond those available to nonprivileged accounts. A privileged account is not necessarily any account that can "affect a material change to the technical or business operations of the covered entity" ((l)(2)). Without any limitation on the scope of covered privilege accounts, this definition would encompass thousands of accounts that engage in hundreds of thousands of actions. The definition should be narrowed. Covered entities must be able to implement a risk-based approach to monitoring privileged accounts in conjunction with other controls to protect information systems and facilitate resiliency, which is contemplated under section 500.14 of the amendment.

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. (APC, p. 17)

Cyber program testing/scanning and vulnerability management (section 500.5). The proposed revisions to this section would impose more prescriptive obligations on covered entities, including requiring annual (1) independent penetration testing and (2) vulnerability assessment scanning. Class A companies/covered entities should have flexibility to conduct penetration testing internally without a mandated reliance on an external independent provider. Covered entities should be able to make their own risk-based determination of an appropriate time frame for vulnerability scanning and not default to biannual scanning per the amendment.

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. (APC, pp. 38–39)

Section 500.5(d) would require a covered entity to document material security issues (e.g., security vulnerabilities) found during testing and report them to its senior governing body and senior management.

Although it is appropriate that senior management should receive such reports, it should not be necessary for the board to receive these reports whenever vulnerabilities are identified. If DFS determines that it is necessary to include such discoveries in a board report, this provision should be added to the annual CISO report called for in section 500.4. Whether this report goes to senior management or the board, the language should be refined to only require the reporting of material issues that are not remediated in accordance with Part 500 remediation guidelines. Proposed changes follow:

DRF amendment

(d) document material issues found during testing and report them to its senior governing body and senior management.

Chamber recommendation

(d) document material issues found during testing and report material issues that have not been remediated in accordance with remediation guidelines.

Further, any requirements related to patching and managing vulnerabilities should be developed in a manner consistent with CISA binding operational directives (e.g., BOD 20-01);[22] and industry best practices and international standards (e.g., International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 30111 and 29147) for coordinated vulnerability handling and disclosure or CVD.[23]

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

[22] https://www.cisa.gov/binding-operational-directive-20-01

[23] CISA, "New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks," November 16, 2021. https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

It is important to distinguish vulnerability information from incident data. Vulnerabilities are found routinely and mitigated based on industry best practices and international standards for CVD. In general, information concerning vulnerabilities is kept in strict confidence during the CVD process until mitigations are publicly available. This is done to reduce the risk that sensitive information could be exploited by attackers to harm users and the cyber ecosystem.

The practice of maintaining vulnerability information in strict confidence is embodied in international standards for CVD (ISO/IEC 30111, 29147) and endorsed by Congress. See the IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207) and CIRCIA at section 2245(a). https://www.congress.gov/bill/116th-congress/house-bill/1668

to those agencies. Therefore, the Department did not make any changes in light of this comment. (APC, p. 38)

Cybersecurity program risk assessments (section 500.7(b)(2)). The Chamber recommends tailoring the automated blocking of commonly used passwords to assets that are directly owned and managed by the covered entity. Third party applications and services are unlikely to provide for automated methods of blocking commonly used passwords. Due to the volume or use of cloud services by organizations, it is unreasonable for CISOs to approve in writing the use of reasonably equivalent or more secure compensating controls for each affected application or service.

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. (APC, pp. 47–48)

Class A company risk assessments (section 500.9(d)). Class A companies/covered entities should not be subject to a prescriptive requirement with respect to using external experts to conduct a risk assessment. In many cases, it may be appropriate and sufficient for covered entities to conduct risk assessments internally by qualified personnel and rely on external consultants and other service providers for other aspects of implementation and maintenance of their cybersecurity.

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. (APC, pp. 50–53)

Commented [EMJ19]: The Chamber appreciates that DFS intends to remove section 500.9(d). However, with respect to independent audits, the cadence and audit content should be based on the size, complexity, and risk profile/appetite of the covered entity.

Further, if a covered entity is adopting the cybersecurity program of a larger firm, then the covered entity should be able to utilize the same audit cadence and policies and procedures that the larger firm uses.

Third party service provider oversight (section 500.11, etc.). Section 500.11 of the amendment demands numerous requirements concerning the oversight of third party service providers. These prescriptive requirements, however, should be risk based. Part 500 places unreasonable burdens on the relationships between companies and third party organizations, such as vendors.

For example, section 500.11(a)(4) would require that covered entities conduct a "periodic assessment," or seemingly annually under section 500.8(b)), of third parties. However, companies should have greater discretion based on the risk profiles of third parties about when assessments are necessary. The Chamber thinks that it is quite reasonable to argue that businesses should not be compelled to conduct an annual assessment of a third party that it uses just once every two years.

Establishing a cybersecurity program and improving it over time is an optimal cybersecurity strategy for many businesses. Still, the Chamber is concerned that some third party service providers may struggle to meet the costs associated with a vigorous cybersecurity program. Costs may not be an obstacle for some businesses. For others, however, the inability to afford a robust cybersecurity program could mean the loss of business from a covered entity.

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. (APC, pp. 54–55)

Cybersecurity program and encryption (section 500.15). The amendment would require encryption or "alternative compensating controls" that go beyond the encryption requirements under laws such as the Safeguards Rule, which covers nonpublic consumer data. A number of technologies used by financial services companies, such as Confidential Computing, provide additional protections that may be appropriate and extend beyond encryption to safeguard data both in transit over external networks and at rest. The Chamber supports flexible and technology-neutral approaches to security.

The amendment to Part 500 would require the encryption of all nonpublic information—unless it is infeasible, in which case companies may apply effective alternative controls. Covered entities should be able to encrypt data or apply an alternative control(s)

based on an assessment of risk, rather than on what is feasible or infeasible. This would help ensure that the costs and the security benefits of the controls are proportionate to the risks.

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. (APC, pp. 66–67)

Incident response planning (sections 500.16). Sections 500.16, in part, impose incident response requirements on covered entities. The response provisions are overly broad. For instance, section 500.16(a)(v) calls for regulated businesses to remediate "any identified weaknesses" in information systems and associated controls. Such thinking, on the surface, seems logical but is out of step with managing risks and threats based on prioritizing threats.

BCDR and the availability/functionality of a covered entity's services (section 500.16(a)(2)). It is positive that DFS recognizes the importance of the materiality standard to some cybersecurity issues. Still, the Chamber urges DFS to add a materiality threshold to a BCDR provision to focus compliance activities of covered entities. The Chamber's recommended edit would convey that BCDR planning should focus on the availability and functionality of material services in the proposed section 500.16(a)(2).

Chamber recommendation

(2) Business continuity and disaster recovery plan (for purposes of this Part, BCDR plan). BCDR plans shall be reasonably designed to ensure the availability and functionality of the covered entity's material services and protect the covered entity's personnel, assets and nonpublic information in the event of an emergency or other disruption to its normal business activities. Such plans shall, at minimum: ...

Moreover, the Chamber believes additional tailoring would better balance a CISO's day-to-day responsibilities and his/her reporting duties to company officials. Also, a covered entity may or may not be equipped to ensure that all of its services are operational in the wake of a cyber incident. DFS should place greater emphasis on a covered entity's material services.

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. (APC, pp. 72–73)

BCDR plan distribution (section 500.16(b)). The vague requirement to distribute BCDR plans to all "necessary" employees could be impractical and create undue complexity, including document management and security challenges. Covered entities should be able to maintain discretion on how they handle access to and the distribution of relevant policies and procedures.

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. (APC, p. 74)

Annual incident response plan testing (section 500.16(d)). Covered entities should have flexibility to determine appropriate participants for incident response plan testing, such as through tabletop exercises. Senior officers, including the "highest-ranking executive" or CEO of the covered entity, may not be a necessary participant in such exercises, and they should not be required to attend every annual exercise.

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. (APC, p. 72)

Commented [EMJ20]: DFS is urged to make available an option for the highest-ranking executive of the covered entity to have a delegate participate in incident and BCDR testing regardless of its frequency. Requiring the highest-ranking executive to participate in seemingly all of the testing is unnecessary and would be burdensome if conducted annually.

DFS "acknowledges that the CEO does not need to be involved in all of testing or participate in all of the exercises," but this is not what the text of the regulation language says.

Section 500.16(d) states:

"(d) Each covered entity shall periodically, but at a minimum annually, test its:

(1) incident response and BCDR plans with all staff critical to the response, including senior officers and the **highest-ranking executive** [bolding added] at the covered entity, and shall revise the plan as necessary; and. …" (p. 14)

Notice of cybersecurity events and extortion/ransomware payments (section 500.17(c)). The Chamber is concerned that the new notice-and-explanation requirements relating to extortion payments (see subsection (c)) would create undue risk and unnecessary complexity for covered entities, as well as create conflicting obligations for covered entities to the extent that they engage with law enforcement agencies in making a ransomware/an extortion payment.

The Chamber strongly recommends either eliminating subsection (c)(2) or providing more flexibility to the requirement to engage federal authorities before making a ransomware payment. While consulting with federal entities may seem straightforward, businesses that have extensive relationships with CISA, law enforcement, and the Department of the Treasury tell us that these interactions frequently prove challenging, especially under the short timelines of a ransomware attack. In particular, the requirement to consult with the Office of Foreign Assets Control, which the amendment strongly implies, could add significant time to the due diligence process with little benefit to a company's security and resilience.

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. (APC, p. #)

Section 500.17(b)(1)(i)(b) of the proposed amendment could be interpreted to require regulated clients to provide DFS with documentation about their suppliers' security practices to certify their compliance with the cybersecurity rules.

(1) Annually each covered entity shall submit to the superintendent electronically by April 15 either:

(i) a written [statement covering] certification which:

(a) certifies that, for the prior calendar year, [. This statement shall be submitted by April 15 in such form set forth as Appendix A of this Title, certifying that] the covered entity [is in compliance] complied with the requirements set forth in this Part[.]; and

(b) shall be based upon data and documentation sufficient to accurately determine and demonstrate such full compliance, including, to the extent necessary, documentation of officers, employees, representatives, outside vendors and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules or otherwise; or ...

Section 500.1(r) would define the term "third party service providers" as follows:

[(n)] (r) *Third party service provider(s)* means a person that:

(1) is not an affiliate of the covered entity;

(2) is not a governmental entity;

(3) provides services to the covered entity; and

[(3)] (4) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity.

Section 500.11 creates specific requirements for managing third party service providers. The term "vendors" is only used three times in the proposed amendment, but this term is undefined by Part 500. The reference to "outside vendors" in section 500.17(b)(1)(i)(b) could be interpreted broadly to include "third party service providers" and other types of entities (e.g., third party auditors and certification organizations).

A company told the Chamber, "Generally, the confidentiality provisions of our contracts are designed to prevent our clients from disclosing information [company] shares about our security practices. But this requirement could be interpreted to legally require our clients to submit this information to [DFS]."

The Chamber believes that DFS should strike the reference to "outside vendors" from section 500.17(b)(1)(i)(b) of the proposal. Alternatively, DFS should define the term "vendors" to clarify that the amendment would not require regulated clients to share documentation about their "third party service providers." For example, a vendor could be defined as a third party auditor or certification organization hired by the regulated client (i.e., a covered entity) to assess its security compliance but exclude suppliers defined as a third party service provider.

Chamber recommendation

Section 500.17 should be amended as follows:

(1) Annually each covered entity shall submit to the superintendent electronically by April 15 either:

(i) a written [statement covering] certification which:

(a) certifies that, for the prior calendar year, [. This statement shall be submitted by April 15 in such form set forth as Appendix A of this Title, certifying that] the covered entity [is in compliance] complied with the requirements set forth in this Part[.]; and

(b) shall be based upon data and documentation sufficient to accurately determine and demonstrate such full compliance, including, to the extent necessary, documentation of officers, employees, representatives, ~~outside vendors~~ and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules or otherwise; or …

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." (APC, p. 83)

Notice of compliance/annual certifications (section 500.17(b)(2)). The Chamber does not think that DFS should modify the status quo with respect to the certification to expressly require that it be completed by the covered entity's CEO and its CISO.

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. (APC, pp. 84–85)

Enforcement/penalties (section 500.20). It should not be a violation of law to suffer an information security incident or otherwise be attacked by a criminal enterprise, including a state-sponsored organization. The Chamber strongly opposes the penalty provisions proposed in section 500.20.

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. (APC, p. 88)

Commented [EMJ21]: The important, yet missing, policy response is the inclusion of safe harbor provisions for compliant covered entities.

***

Thank you for the opportunity to provide DFS with comments on the amendment to the cybersecurity regulation. If you have any questions or need more information, please do not hesitate to contact me at meggers@uschamber.com.

Sincerely,

Matthew J. Eggers
Vice President, Cybersecurity Policy
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

Appendix [B]

A Balanced Cyber Blueprint for Enhanced Security and Resilience

DFS should hold off on completing its proposed amendment to Part 500 or the cybersecurity regulation. From a practical standpoint, DFS is making the enhancement of covered entities' cybersecurity much more difficult than it needs to be—both for the Department and regulated parties. Indeed, financial services firms are perhaps the most regulated critical infrastructure sector when it comes to cybersecurity.[24]

If DFS believes that an amended cybersecurity regulation would deliver the cybersecurity benefits that its proposal suggests, then the cybersecurity regulation should include strong liability protections for covered entities.

	Self-certification by covered entity	**Certification based on independent audit[25]**
Type of liability protection	*Affirmative defense* against DFS penalties or certain causes of action arising from breach of a device or system security	*Indemnification* against DFS penalties or certain causes of action arising from breach of a device or system security
Type of cybersecurity program	Globally accepted, industry-led program; state or federal cybersecurity regulation; or Part 500	Globally accepted, industry-led program; state or federal cybersecurity regulation; or Part 500

The amended cybersecurity regulation would require covered entities to certify compliance with all sections of Part 500. Such certifications should come with liability protections, ranging from an affirmative defense to indemnification based on the level of certification that a covered entity undertakes. Liability protections should also extend to lawsuits generated by malicious cyber activity.

Such thinking is fair, and it strives for correctness. First, businesses contend with relentless, state-sponsored cyberattacks but lack effective government protection. Justice—or a basic sense of fairness—recommends liability protections for businesses. Second, the

[24] Testimony of Christopher F. Feeney, President, BITS/Financial Services Roundtable (now the Bank Policy Institute), Senate Homeland Security and Governmental Affairs Committee, full committee hearing on "Cybersecurity Regulation Harmonization," June 21, 2017. https://www.hsgac.senate.gov/hearings/cybersecurity-regulation-harmonization

[25] DFS' amendment would require class A companies to implement additional cybersecurity controls, such as conducting independent audits of their cybersecurity programs at least annually.

Department's new proposal would amount to a regulatory free lunch. If DFS believes that new cybersecurity rules would deliver the security benefits the amendment suggests, the Department should confidently pair any revised rules with legal liability protections.

Policymakers should stand behind the perceived correctness of their regulations. Anything short of clear liability protections for covered entities would call into question the assumption that the cybersecurity requirements are appropriately risk based, technically sound, and workable.

The Chamber has a cybersecurity policy blueprint that would encourage businesses to invest in cybersecurity and resilience, which would ultimately better protect data and devices and reduce cybersecurity incidents. To begin with, in addition to Part 500, covered entities should be provided a list of cybersecurity frameworks, standards, regulations, and industry-led efforts to comply with or certify in order to qualify for liability protections.

Businesses Need Flexibility Regarding Compliance

While far from a comprehensive listing, DFS should deem that the following cybersecurity best practices, frameworks, standards, and programs satisfy the cybersecurity regulation's certification requirement:

- The Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST).
- NIST special publication 800-171.
- NIST special publications 800-53 and 800-53a.
- NIST special publication 800-218.
- NIST profile of the Internet of Things Core Baseline for Consumer IoT Products (NIST Internal Report 8425).
- Cybersecurity Maturity Model Certification.
- The Federal Information Security Modernization Act of 2014.
- Title V of the Gramm-Leach-Bliley Act of 1999, as amended.
- Health Information Technology for Economic and Clinical Health (HITECH) Act.
- The Security Assessment Framework for the Federal Risk and Authorization Management program (FedRAMP).
- The ISO/IEC 27000 family, information security management systems.

- The ISO/IEC 30111 and 29147, coordinated vulnerability handling and disclosure.
- Critical Security Controls for Effective Cyber Defense developed by the Center for Internet Security.
- The Profile developed by the Cyber Risk Institute.
- The Payment Card Industry Data Security Standard, as administered by the Payment Card Industry Security Standards Council.

Missing from DFS' proposed requirements are safeguards for businesses that demonstrate their use of existing cybersecurity programs to meet the requirements of Part 500 or a comparable one. Covered entities with cybersecurity programs that reasonably align with these and other laws and regulations that contain cybersecurity requirements should be entitled to liability protections. DFS needs to balance regulatory compliance with greater flexibility in meeting industry-recognized standards, as well as positive incentives to increase the economic security of covered entities, New York State, and the U.S.

It is frequently overlooked that industry is the main force shouldering the protection and resilience of U.S. information systems against cyberattacks initiated by predatory nation-state hackers and other illicit groups. The current regulatory model is unsustainable. It is past time for businesses to get legal credit when they meet certain security standards, including regarding enterprise risk management and IoT devices.[26]

There is a clear surplus of agency regulators vis-à-vis agency defenders at the state and federal levels. This mismatch has profound implications for U.S. security. Regulatory agencies are free to pass judgment on businesses that are cybercrime victims. Yet these businesses are often unsupported against international criminal gangs and purveyors of ransomware. Consider the role of law enforcement.

The FBI and the Secret Service are just two federal entities—compared with the Cybersecurity Forum for Independent and Executive Branch Regulators (the Cyber Forum), which is made up of 17 departments and agencies—that push back on malicious actors.[27]

---

[26] See the Chamber's October 18, 2021, comment letter to the Federal Communications Commission (FCC) on the agency's notice of inquiry regarding ways to strengthen IoT cybersecurity. https://www.fcc.gov/ecfs/file/download/211018_Comments_IoT%20Cybersecurity%20SecureEquipment_FCC.pdf?folder=10182049018274

[27] The federal Cyber Forum includes the following agencies: the Coast Guard, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, CISA, the Department of Health and Human Services, the Department of Homeland Security, the Department of the Treasury, FCC, the Federal Energy Regulatory Commission, the Federal Housing Finance Agency, the Federal Reserve Bank, FTC, the Food and Drug Administration, NIST, the Nuclear Regulatory Commission, the Office of the Comptroller of the Currency, and SEC. https://www.meritalk.com/articles/fcc-chair-rosenworcel-to-lead-relaunched-interagency-cyber-forum

In addition, the amendment appears to reject the growing consensus that agencies need to work together, in collaboration with industry, to achieve greater consistency in cybersecurity requirements. Today, there is considerable fragmentation across agency jurisdictions and sectors.[28] What is more, fragmented approaches to cybersecurity lead to duplicative and/or confusing security requirements, splinter organizations' risk management budgets, consume precious time, and draw cyber talent away from defending against cyberattacks.

DFS should pause the promulgation of its amendment to the cybersecurity regulation and work with industry to advance balanced and innovative cybersecurity rules that achieve the Department's objectives, are better harmonized with other state and federal laws/regulations, and protect covered entities from liability.

https://www.fcc.gov/document/chair-rosenworcel-remarks-cybersecurity-forum-principals-meeting

[28] The national cyber director's (NCD's) October 2021 strategic statement places much emphasis on cybersecurity cooperation and coordination across the many public, private, and international stakeholders in the ecosystem.

The White House, Office of the National Cyber Director, *A Strategic Intent Statement for the Office of the National Cyber Director*, October 2021, p. 7.
https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf