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.[1]

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.

[1] 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[2] the multiple cybersecurity rules that businesses must comply with—and the list continues to increase.[3] Due to the pronounced lack of harmonization, businesses face a number of challenges.

---

[2] 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

[3] 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 the Appendix.)

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.[4]

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 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.

---

[4] 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

- 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.

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.[5]

- 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.

---

[5] Raymond J. Decker, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T, U.S. Government Accountability Office, October 12, 2001. https://www.gao.gov/products/gao-02-150t

- 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.[6]

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 5001.17 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.

---

[6] 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

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.[7]

2.1.2. A logical place to start is the bipartisan Cyber Incident Reporting for Critical Infrastructure Act of 2022 (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 the Cybersecurity and Infrastructure Security Agency's (CISA's) request for information on implementing the law.[8]

- **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.

- **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.

---

[7] 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

[8] Sara Friedman, "U.S. Chamber encourages CISA to seek 'qualitative' information in [supplemental] incident reports under upcoming mandatory regime," *Inside Cybersecurity*, November 30, 2022. https://insidecybersecurity.com/daily-news/us-chamber-encourages-cisa-seek-%E2%80%98qualitative%E2%80%99-information-incident-reports-under-upcoming

- 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.

- 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.

- 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.

***

Section 500.17 (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.

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.[9]

[9] 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

- 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."[10]

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

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)]

[10] PPD 41, *United States Cyber Incident Coordination*, July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

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 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.

- 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.[11] 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.[12]

- 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.[13]

- 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

---

[11] 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

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

[13] 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

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.[14]

> 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

[14] 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

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. ...

- 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.

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.[15] 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.[16]

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.[17] 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.

---

[15] 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

[16] 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

[17] 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

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.

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.

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.

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 Cybersecurity and Infrastructure Protection Agency (CISA) binding operational directives (e.g., BOD 20-01);[18] 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.[19]

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.

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

[19] 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

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.

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.

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.

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.

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.

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.

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.

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 ...

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.

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.

***

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

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.[20]

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[21]**
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

[20] 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

[21] 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.[22]

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.[23]

---

[22] 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

[23] 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.[24] 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

[24] 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