November 14, 2016

Via CyberRegComments@dfs.ny.gov

Cassandra Lentchner
Deputy Superintendent for Compliance
New York State Department of Financial Services
One State Street
New York, NY 10004

Subject: New York State Department of Financial Services' proposed *Cybersecurity Requirements for Financial Services Companies*

Dear Ms. Lentchner:

The Business Council of New York State, the Electronic Transactions Association (ETA), the Property Casualty Insurers Association of America (PCI), and the U.S. Chamber of Commerce, which represent nearly every sector of the U.S. economy, welcome the opportunity to respond to the New York State Department of Financial Services' (the DFS') proposed *Cybersecurity Requirements for Financial Services Companies* (the Proposal).[1]

Cybersecurity is a leading priority for the U.S. business community, from automobile companies to water utilities. Financial services firms, in particular, expend significant resources annually to safeguard consumer data, protect against cybercrime, and enhance the resilience of their infrastructure.[2] Businesses work diligently to stay a step ahead of illicit actors by employing sound risk-management principles. Over the past several years, the business community has worked constructively with the Obama administration, Congress, and other stakeholders on cybersecurity initiatives that offer positive and cooperative solutions to increasing the safety and soundness of U.S. institutions.

A particularly noteworthy achievement is the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework), which many private-sector organizations use and promote widely and enthusiastically.[3]

Our organizations are concerned that the Proposal would establish yet another cybersecurity regime in a long line of prescriptive policies impacting industry, not only domestically but internationally.[4] It would impose new requirements on companies within an environment of preexisting and overlapping federal and state cyber- and data-security rules.

Indeed, the Proposal, especially Section 500.3, Cybersecurity Policy, would foist significant cybersecurity mandates on financial companies in several areas, from information

security to incident response and more. The Proposal, like so many public policies concerning cybersecurity, does not sufficiently recognize the potentially extraordinary costs that industry faces in creating and maintaining robust information-security programs.

Industry and leading U.S. officials do not believe that more regulations—whether at the international, federal, or state and local levels—will lead to stronger cybersecurity. What is noteworthy, Secretary of Commerce Penny Pritzker voiced on September 27 at the Chamber that public-private collaboration needs to be deepened, not damaged. We believe that this Proposal would benefit from additional collaboration with industry so that it reflects the interests of government and businesses and the operational requirements of many cybersecurity programs.

Secretary Pritzker said that cyberattacks cannot be handled solely by the U.S. government. Yet cyberspace is the "only domain where we ask private companies to defend themselves" against foreign powers and other significant threats. She wondered aloud, "Does that sound as crazy to you as it does to me?" Indeed, government does not stand between private entities and malicious hackers. The Secretary noted, too, that federal laws and regulations are unable to keep pace with rapidly evolving cyber threats. "No static checklist, no agency rule, no reactive regulation is capable of thwarting a threat we cannot foresee." A core problem, she observed, is that relationships between businesses and regulators are "inherently adversarial," not collaborative, and this inhibits sound security.

Our groups hold that the Proposal, as currently drafted, would represent a substantive setback for effective cybersecurity and public-private collaboration. The proposed measure would also negatively affect both financial and nonfinancial firms by setting a misguided precedent for other states to follow.

BIG PICTURE: IT'S IN POLICYMAKERS' AND INDUSTRY'S INTERESTS TO COLLABORATE AGAINST BAD ACTORS

Don't move toward regulation and away from the Framework; the Framework is a sound baseline for businesses' cybersecurity practices

Our associations believe that most businesses and policymakers see the Framework as a key *pillar* for managing enterprise cybersecurity risks and threats, including at home and increasingly abroad. NIST did an admirable job convening industry to develop the Framework over the course of many months. We will press the next administration to embrace the Framework. Our organizations see the Framework as a multistakeholder tool, as a collaborative process, and as a constructive mind-set. Our groups urge private organizations—from the C-suite to the newest hire—to commit to robust cybersecurity practices.

To sustain the momentum behind the Framework, we believe that both industry and government have jobs to do. On the one hand, our associations, especially the Chamber, have been actively promoting the Framework since it was released in 2014. The Chamber's national cybersecurity campaign is funded through members' sponsorships and the financial and in-kind contributions of state and local chambers of commerce, other business organizations, and academic institutions. Further, our organizations' members are using the Framework and urging business partners to manage cybersecurity risks to their data and devices. Industry is working

with government entities, including the Federal Financial Institutions Examination Council and the Department of Homeland Security, to strengthen businesses' information networks and systems against a dizzying array of malicious actors.[5]

Policymakers at all levels of government need to prioritize harmonizing cybersecurity regulations with the Framework

On the other hand, our groups urge policymakers at all levels of government to help agencies and departments *harmonize* existing regulations with the Framework and maintain the Framework's voluntary nature. 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 Proposal overlaps and conflicts with existing cybersecurity requirements and guidance, particularly at the federal level. Layering on another, quite different cybersecurity regime would steer organizations' resources toward compliance and confuse them about what standards, guidance, and best practices they are supposed to follow and document. The DFS is moving fairly swiftly on a top-down, complicated rulemaking that would benefit from lengthier, in-depth scrutiny. The Proposal would likely undermine the bottom-up, collaborative approach to cybersecurity policy that many industry organizations, including the Chamber, are advancing with government partners domestically and overseas.[6]

In addition to urging regulatory harmonization, our organizations oppose the creation of new or quasi-cybersecurity regulations, especially when government authorities have not taken affected entities' perspectives into account. We believe that the DFS needs to dramatically pull back on this rulemaking and involve itself in a more in-depth consultative process with affected entities.

Above all, the DFS rulemaking represents the opposite approach to shared, cooperative public-private cybersecurity that the Obama administration and our associations are holding up as a model for stakeholders to imitate. The Proposal represents the development of an entirely new and distinct set of standards that overlap and conflict with other comprehensive cybersecurity requirements and governance frameworks.

The Proposal is prescriptive; effective cybersecurity requires managing risks

Our organizations believe that the proposed rulemaking is overly prescriptive. There is a strong consensus among security professionals that effective approaches to cybersecurity should be risk-management centric. The Proposal fails to incorporate a risk-based approach that can adapt over time to account for changes in technology and the ever-changing cybersecurity threat landscape.

Cyber actors constantly adjust their tactics, techniques, and procedures to defeat businesses' defenses. Effective cybersecurity requires organizations to adapt to a constantly changing and menacing environment. Potent cybersecurity requires a concerted team effort. Government officials should work with industry leaders, technical experts, and information security professionals to manage cyber risks and threats. Firms must improvise and dedicate resources in real time to combat myriad threats.

We contend that the DFS' proposed rules demand prescriptive and rigid actions that fail to take into account the actual risks faced by the business community. Firms of all sizes handle a range of information types and must manage different networks that come with varying degrees of risks. The blind application of cybersecurity controls, while notionally easier to track by agency examiners, would not deliver effective protection for "Covered Entities" (Section 500.01(c)). An underlying risk calculus must be the primary driver for what information security controls to select and implement.

Our groups encourage the DFS to take its lead from the Framework, which is intended to be flexible and adaptive. As business models and threats change, the DFS must allow protections to adjust quickly to an evolving landscape. By requiring the implementation of specific controls and activities, the Proposal would invariably force a uniform and inappropriate cybersecurity program on an array of uniquely situated financial companies.

PRELIMINARY VIEWS ON ELEMENTS OF THE PROPOSAL

This portion of the letter addresses our associations' initial views on various sections of the Proposal. The DFS suggests that the Proposal is not "overly prescriptive," but we count approximately 43 "shalls" in the span of 11 pages. Top-down mandates could have a debilitating impact on a company's cybersecurity, which we reject.

- **Third-Party Oversight (Section 500.11).** Section 500.11 of the Proposal demands numerous requirements concerning third-party vendors. These requirements, however, should be risk based. The draft Proposal would place unreasonable burdens on the relationships between companies and third-party organizations, such as vendors.

  For example, Section 500.11(a)(4) would require that entities conduct a "periodic assessment, at least annually," of third parties. However, companies should have greater discretion, based on vendors' risk profiles, about when assessments are necessary. We think 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, our organizations are concerned that some third-party companies may struggle to meet the costs associated with a vigorous information-security program. The expense of such programs should not be overlooked. Costs may not be an obstacle for some companies. For other companies, however, the inability to afford a robust cybersecurity could mean the loss of business from a Covered Entity, which is not constructive and probably not the intent of the Proposal's authors.

  Also, Section 500.11(b)(2) directs that companies "use encryption to protect Nonpublic Information in transit and at rest," but this is not practical in every circumstance. While we support strong encryption, mandating the encryption of all data is simply not practicable and would interfere with the legitimate operations of regulated companies. Requiring all vendors to encrypt Nonpublic Information (Section 500.01(g)) would

constitute a costly and technical undertaking, which is not a realistic solution to stronger information security in every situation.

- **Data Retention (Section 500.13).** Section 500.13 dictates companies' data retention policies and procedures. Our groups believe that the DFS should eliminate this section of the Proposal. As constructed, data retention and destruction activities would become compliance functions. We think that data preservation processes should be governed by the records retention policies of businesses, which set forth the holding period for various categories of data. The mandated disposal of any Nonpublic Information would be unduly burdensome in many circumstances because of the manner in which information is maintained and intermingled among multiple networks and systems.

  Further, data can easily be required for business purposes beyond what is "necessary for the provision of the products or services for which such information was provided to the Covered Entity." For example, a customer application may not seem "necessary" for the provision of relevant financial services and products, but it is necessary as evidence of authorized activities.

  Like so much of the Proposal, Section 500.13 takes a one-size-fits-all approach to structuring security programs, whereas a risk-based focus would serve the cause of information security much better.

- **Training and Monitoring (Section 500.14).** Section 500.14 of the Proposal would "require all personnel to attend regular cybersecurity awareness training sessions," which seems sensible on the surface. Our associations support greater cybersecurity awareness among businesses and employee education. However, in practice, the training sessions could become rigid, unenthusiastic exercises that dictate specific roles and responsibilities for companies' personnel.

  State-based rules could easily zero out financial firms' discretion about training and spread thinly the resources that they need to adapt to a changing threat environment. Businesses are in the best position, working collaboratively with government officials, to understand how personnel need to be trained and monitored. New York officials should help industry with enhancing cybersecurity training rather than dictating how it is done.

- **Incident Response Plans, Reporting (Sections 500.16 and 500.17).** Sections 500.16 and 500.17 impose information-security response, reporting, and notice requirements. The response provisions are overly broad. For instance, Section 500.16(b)5) calls for regulated businesses to remediate "any identified weaknesses" in information systems and associated controls. Such thinking, on the surface, seems logical but is wildly out of step with managing risks and threats based on prioritizing threats. Companies that must remediate all weaknesses equally would end up fixing poorly the ones that matter most.

  The reporting requirements are seemingly all-encompassing. First, the term "Cybersecurity Event" (Section 500.01(d)) includes comparatively minor incidents (e.g., pings) to significant attacks of an organization's information system.

Second, companies must notify the Superintendent of Financial Services of any Cyber Event that "has a *reasonable likelihood* of *materially affecting* the *normal operation* of the Covered Entity or that *affects* Nonpublic Information" [italics added]. By the time business principals figure out what "reasonable likelihood," "materially affecting," and "normal operation" mean in the context of the Proposal, they'll perhaps conclude that they have to report more, not less, information. Our organizations seriously question the quality that such information would offer regulators. Most savvy cybersecurity professionals would view the flood of data to be unusable "noise" as opposed to actionable threat data.

Third, notification to public authorities under Section 500.17 should only be triggered by events that have a significant risk of material harm—a higher threshold than "materially affecting." In our associations' experience, not every cyber incident that involves Nonpublic Information or a company's operations needs to be reported. Among other things, the term "Cybersecurity Event" needs to be calibrated to better match today's cyber realities. Under the Proposal's draft definition, even unsuccessful "attacks"—of which there are millions of incidents daily across the financial industry—would trigger the notification requirement. Massive reams of notifications are not something the DFS should want to get.

Fourth, if the DFS requires notifying state officials, it should align the requirement with existing data-breach notification requirements. These requirements exist in 47 states.[7] New York law requires notification for any individual whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.[8] New York rules also specify what is considered "private information," and they are designed to address information that may cause harm if released. The Proposal's notification requirements, in contrast, are much too broad.

Industries like financial services and health care already operate under breach notification regulations. Creating another, likely conflicting definition concerning the breaching of Nonpublic Information would add to the regulatory burden that companies face in the aftermath of an attack. Businesses should devote their time and energy to mitigating cyber incidents. The accumulation of red tape leads to a diffusion of smart cybersecurity response efforts.

The requirement to notify the Superintendent within 72 hours "after becoming aware of a Cybersecurity Event" is unrealistic. No state or federal agency requires notification within such a short period of time. It often takes days, if not weeks, to investigate incidents. Imposing a rigid requirement to provide notice to the DFS in the middle of a response effort would hamper firms in unproductive ways.

There is also no delay, or carve-out, provision for working with law enforcement. In many instances, firms must immediately coordinate with law enforcement in responding to an attack, and law enforcement may request that notice not be provided to third parties. The DFS should revise its rule to permit delaying notification in such instances. The FBI

and the Secret Service wrote to a federal agency this past summer and said that companies should be able to "delay customer notification if, in the judgment of the federal law enforcement agency, the notification would interfere with a criminal or national security investigation."

The law enforcement entities went on to say that in exceptional circumstances, the FBI and the Secret Service may conclude that customer notification would "reveal sensitive sources or methods or otherwise impede the ability of the agency to conduct a law enforcement investigation. This would especially be the case in national security matters, where the FBI might determine that providing notice of the data breach or the scope of the breach could harm U.S. national security. . . ."[9] The Proposal needs to account for some business partnerships with law enforcement.

- **Technical Requirements (Sections 500.12 and 500.15).** The Proposal mandates specific testing and technical requirements, including multifactor authentication, and encryption of Nonpublic Information. Our organizations agree that protecting sensitive business and consumer data is central to most robust cybersecurity programs. Yet, as written, the section's requirements are overly generalized and should be technology neutral.

  It is our groups' belief that cyber programs must be flexible to enable entities to adapt their defenses and measures to address existing threats, which constantly evolve. The Proposal should be amended to clearly recognize each entity's special risk profile. No specific technologies should be required.

Our associations' position is to oppose top-down regulations coming from agencies and departments—but not for its own sake. Businesses share the goal of mitigating cybersecurity risks and are committing billions of dollars to the security and resilience of their enterprises.

Most observers agree that regulations cannot possibly keep pace with bad actors and would lead to check-the-box security mandates that are costly, time-consuming, and ineffective—thus pulling businesses' limited resources away from cybersecurity and toward compliance. Such an outcome would harm both the nimbleness needed by companies to respond to incidents as well as public safety—it's the exact opposite effect that the Framework initiative is trying to achieve.

Our organizations appreciate the DFS's consideration of the issues that are highlighted in this letter.

Sincerely,

The Business Council of New York State
Electronic Transactions Association (ETA)
Property Casualty Insurers Association of America (PCI)
U.S. Chamber of Commerce

Notes

[1] www.dfs.ny.gov/legal/regulations/proposed/propdfs.htm, www.governor.ny.gov/news/governor-cuomo-announces-proposal-first-nation-cybersecurity-regulation-protect-consumers-and

[2] www.nist.gov/sites/default/files/may_16_2016_nyc_meeting_minutes.pdf

[3] http://csrc.nist.gov/cyberframework/rfi_comments_02_09_16.html

[4] See the Chamber-led March 11, 2016, group letter to the European Commission (EC). The EC requested stakeholders' views on cybersecurity public-private partnerships. The letter, signed by 19 industry associations, argues that embracing the Framework approach could advance the EU's goals for cybersecurity and a Digital Single Market. www.uschamber.com/sites/default/files/documents/files/industry_comment_ltr_to_european_commission_on_future_of_public_private_partnerships.pdf

[5] www.ffiec.gov/cybersecurity.htm

[6] "Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks" (December 10, 2015). UC Davis *Business Law Journal*, 2016; Kelley School of Business Research Paper No. 16–2. http://ssrn.com/abstract=2702039

[7] Existing federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the Gramm-Leach-Bliley Act (GLBA), impose security and breach notification requirements on specific industries or types of data. Additionally, 47 states, the District of Columbia, and 3 territories have enacted laws requiring breach notification, while at least 12 states have enacted data security laws, designed to reduce the likelihood of a data breach. Alabama, New Mexico, and South Dakota have not enacted breach notification laws. www.fas.org/sgp/crs/misc/R44326.pdf

[8] N.Y. Gen. Bus. Law. Section 899-aa (1)(b). http://codes.findlaw.com/ny/general-business-law/gbs-sect-899-aa.html

[9] www.fcc.gov/ecfs/filing/107052845130219/document/10705284513021926 76