Morgan Lewis

Mark L. Krotoski
Partner
+1.650.843.7212
mark.krotoski@morganlewis.com

Charles Horn
Partner
+1.202.739.5951
charles.horn@morganlewis.com

January 27, 2017

VIA EMAIL: CyberRegComments@dfs.ny.gov

Maria T. Vullo, Superintendent
New York State Department of Financial Services
One State Street
New York, NY 10004-1511

Dear Superintendent Vullo:

We appreciate the opportunity to comment on the New York State Department of Financial Services' ("DFS's") re-proposed regulatory framework titled "Cybersecurity Requirements for Financial Services Companies" (the "Supplemental Proposed Rules").

On September 13, 2016, the DFS issued a set of proposed rules, described as "a new first-in-the-nation regulation".[1] After the first comment period closed on December 28, 2016, the DFS revised its Proposed Rules and delayed the effective date until March 1.[2] The Supplemental Proposed Rules would require banks, insurers, and other DFS-supervised financial services companies to adhere to stringent cybersecurity requirements mandating firms to test their systems, establish plans to respond to cybersecurity events, and annually certify compliance with the cybersecurity requirements, among other mandates.

We had previously commented on the first set of proposed rules; our comment letter is attached as Appendix A, and we welcome the opportunity to offer our suggestions to enhance the Supplemental Proposed Rules in this comment letter.

---

1 *See* Press Release; Governor Cuomo Announces Proposal Of First-In-The-Nation Cybersecurity Regulation To Protect Consumers and Financial Institutions (Sept. 13, 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf; *see also* New York State Department Of Financial Services Proposed 23 NYCRR 500, Cybersecurity Requirements For Financial Services Companies, *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

2 *See* Press Release; DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers And Financial Institutions (Dec. 28, 2016), *available at* http://www.dfs.ny.gov/about/press/pr1612281.htm; *see also* New York State Department Of Financial Services Proposed 23 NYCRR 500, Cybersecurity Requirements For Financial Services Companies, available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

We appreciate the steps that the DFS took to revise its proposal in response to comments received. In particular the ability of Covered Entities to base their cybersecurity policies and other required activities on the basis of a risk assessment provides useful flexibility to Covered Entities under the re-proposed regulations. That said, we believe that there remain several areas of the Supplemental Proposed Rules that the DFS can improve upon and so we submit our recommendations as noted below.

In general, some questions that should be considered include whether the objective to promote meaningful cybersecurity by Covered Entities can best be accomplished through guidance or voluntary standards. Also, consideration should be given to the costs and burdens are imposed by the proposed regulation, particularly given limited resources of Covered Entities and other choices that may be better tailored to promote effective cybersecurity.

Much of the proposed rule is "first in the nation" because the regulation would establish new and inconsistent standards that other jurisdictions have not adopted. Consideration should be given to the adoption of existing, flexible standards rather than imposing new, prescriptive standards. Harmonization should be encouraged. Another concern is that the new proposed standards may become obsolete based on new technology and evolving standards that may be better suited to promote meaningful cybersecurity. The mandatory compliance approach in the proposed regulation will foster a "check the box" process, rather than allow Covered Entities to identify and adopt measures that are best suited to their circumstances.

We offer the additional recommendations in your consideration of the new regulation.

I. The Supplemental Proposed Rules Should Allow a More Flexible Framework that Promotes Effective Cybersecurity

The DFS proposes that all firms subject to the Supplemental Proposed Rules ("Covered Entities") would be required to satisfy "minimum" cybersecurity standards, revised to reflect a new risk-based approach to such standards. We welcome the introduction of a risk-based approach because it has the effect of limiting certain requirements and permits Covered Entities to tailor their cybersecurity programs based on their risk assessments, thereby eliminating the one-size-fits-all approach previously introduced. We continue to be concerned, however, that the Supplemental Proposed Rules continue to impose prescriptive mandates, in contrast to a flexible, best-practice approach that the financial industry has widely adopted.

As we previously commented, cybersecurity policies are most effective when they are tailored to a firm's unique cyber risks and vulnerable information.[3] However, the Supplemental Proposed Rules contain several overly prescriptive elements. Proposed Rule 500.05 states:

> The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing **shall include continuous monitoring or periodic penetration testing and vulnerability assessments, and shall be done periodically.**

We would not recommend that the DFS include a requirement to have a specific technical standard, such as penetration testing, which may not be optimal for each Covered Entity and may

[3] Appendix A; Section II.

become obsolete. For example, penetration testing and other system vulnerability assessments are evolving on a continuous basis, making it impracticable to prescribe specific standards that do not run the risk of becoming quickly obsolete. Multi-factor authentication, while appropriate in many circumstances, may be supplanted by other technological safeguards. The objective is to ensure the data is secure. There are a variety of means today, and evolving over time, that may be more adept at protecting the data. The regulation may become outmoded by superior methods.

Therefore, instead of adopting strict mandates, DFS should adopt principles that enable Covered Entities' cybersecurity programs to evolve over time and with advances in technology. A principles-based approach is especially important given that Covered Entities span the spectrum from insurance companies to banks to financial institutions,[4] and gather and retain different types of protected data. The cybersecurity systems vary widely amongst these different types of businesses. In addition, Covered Entities vary greatly in their size and sophistication of business activities.

The DFS's final rules should identify best practices and standards that Covered Entities can tailor to their unique information systems and cyber risks.

II. Any Reporting Requirement Should Be Tied to Meaningful Circumstances Connected with the Cyber Incident and Should Conform with Existing Reporting Requirements

Proposed Rule 500.17 requires a Covered Entity to report a "Cybersecurity Event"—defined as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an Information System[5] or information stored on such Information System"[6] —that has "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" to the DFS within the first 72 hours of a Cybersecurity Event.[7] While the revision of the notification requirement to limit it to the risk of actual and material harm is helpful, the reporting rule continues to reference "Cybersecurity Event", which has not been revised to eliminate the reference to an unsuccessful attempt to gain unauthorized access to a Covered Entity's information systems. As a result, a Covered Entity likely would require legal guidance to obtain certainty on when reporting is required.

---

4 Covered Entities range from banks and trust companies to budget planners, charitable foundations, check cashers, credit unions, domestic representative offices, foreign agencies, foreign bank branches, foreign representative offices, health insurers, accident and related entities, holding companies, investment companies, licensed lenders, life insurance companies, money transmitters, mortgage bankers, mortgage brokers, mortgage loan originators, mortgage loan servicers, New York state regulated corporations, premium finance agencies, private bankers, property and casualty insurance companies, safe deposit companies, sales finance companies, savings banks and savings and loan associations, and service contract providers.

5 The Supplemental Proposed Rules define the term "Information System" to mean "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems." Proposed Rule 500.01(e).

6 Proposed Rule 500.01(d) (Cybersecurity Event Definition) (The term "Cybersecurity Events" is defined as "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".)

7 Proposed Rule 500.17(a) (Notices to Superintendent).

The new standard is not only novel but cumbersome and unworkable. Instead of establishing a novel formulation, consideration should be given to similar standards that are used in other jurisdictions.

In our previous comment letter,[8] we recommended that DFS provide a Covered Entity that is the subject of a Cybersecurity Event the opportunity to focus its efforts on resolving the Cybersecurity Event instead of on compliance with myriad reporting requirements under DFS regulations, state law and federal law. We continue to make that recommendation. We further recommend that DFS eliminate unsuccessful access attempts from the definition of Cybersecurity Event.

III. The New "Confidentiality" Provision is Ambiguous

A. Proposed Rule 500.18 is Ambiguous

Under Proposed Rule 500.18 (titled "Confidentiality"), the intention of the DFS is ambiguous. The provision reads:

> Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

The language of this provision could be interpreted to mean that information provided to DFS hereunder is not subject to disclosure under any other state or federal law, including laws that DFS does not administer or enforce, a reading that would appear to be beyond DFS's authority and could put Covered Entities in conflict with other non-DFS state laws, or federal laws. We therefore recommend that DFS revise this provision to clarify the provision's intent and assure full consistency with other applicable federal or state confidentiality requirements.

B. Additional Confidentiality Protections

DFS should provide that documents related to a risk assessment or other DFS-required records subject to attorney-client privilege but provided to DFS remain subject to the attorney-client privilege under New York law and will not be used for purposes other than the exercise of DFS's regulatory and supervisory duties and responsibilities. Alternatively, the proposed regulation should clarify that it does not require the production of privileged communications.

IV. The Proposed Annual Compliance Certification Should Be Eliminated

Supplemental Proposed Rule 500.17(b) still requires a Covered Entity's board of directors or senior officer to submit to the DFS, on an annual basis, a certification that the Covered Entity is in compliance with the Supplemental Proposed Rules. We had already recommended,[9] and continue to recommend, that the DFS not adopt this requirement in the final rules. Instead of promoting meaningful cybersecurity, the certification required fosters a "check the box" process of compliance. This approach deprives Covered Entities from developing and innovating measures that are best suited to avert cyber risks and protect the data.

---

8 Appendix A; Section III.

9 Appendix A; Section IV.

V. CISO Function

The Supplemental Proposed Rules require Covered Entities to have a CISO; the relevant language reads: "Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, 'Chief Information Security Officer' or 'CISO')." We interpret the revised requirement to mean that a person designated with the title of CISO is not required but, rather one or more individuals may fulfill the "CISO" functions enumerated in the Supplemental Proposed Rules. We respectfully ask the DFS to confirm in the final regulations that this understanding is accurate.

VI. Additional Recommendations

A. The Supplemental Proposed "Substituted Compliance" Rule Does Not Go Far Enough

The DFS provides that a Covered Entity may comply with the Supplemental Proposed Rule by adopting a cybersecurity program maintained by an affiliate, if the affiliate's program: (1) satisfies the DFS requirements; and (2) encompasses the Covered Entity's information systems and nonpublic information. The new provision will benefit firms with multiple subsidiaries subject to DFS oversight, but does not provide substituted compliance to a Covered Entity that is itself already subject to another regulatory requirement that the Covered Entity maintain a cybersecurity program. However, as we explained in our previous comment letter,[10] most Covered Entities are subject to oversight by multiple regulatory authorities. Therefore, we again recommend that the DFS provide for a substituted compliance program whereby Covered Entities subject to other federal or state regulatory requirements that are materially comparable to DFS requirements are not required to also comply with the Supplemental Proposed Rules. The "substituted compliance" will provide greater flexibility to Covered Entities and foster harmonization with existing standards.

B. DFS Should Expand the Exclusion for "Small Firms"

The changes to the limited exemption for "small Covered Entities" under Proposed Rule 500.19 provide useful relief, but we are concerned that the exemption is too narrowly defined to be of real benefit. The exemption only provides relief from a fraction of the Supplemental Proposed Rules and still requires a small Covered Entity to create and maintain a policy regarding access privileges, and policies mandating an annual risk assessment, minimum required clauses for third party service provider agreements, and timely document destruction.[11] A small Covered Entity that falls within the scope of the exemption would still be required to notify the DFS of Cybersecurity Events and is subject to its enforcement authority. The relief, thus, appears to be quite limited in scope.

Further, the limited exemption should provide greater relief from the Supplemental Proposed Rules by exempting small Covered Entities from Supplemental Proposed Rules 500.07 (Access Privileges), 500.11 (Third Party Information Security Policy), 500.13 (Limitations on Data Retention), and 500.17 (Notices to Superintendent - certification).

- A small Covered Entity should not be required to comply with access privileges requirements because, due to a smaller staff, all personnel might have access to

---

10 Appendix A; Section VI.A.

11 Proposed Rule 500.19(a)(3).

all aspects of the small Covered Entity's information systems. This requirement, in practice, would not be useful and could be potentially highly disruptive.

- A small Covered Entity may not have the bargaining power or the resources to retain outside counsel to implement strong cybersecurity provisions in third-party service agreements and, accordingly, should not be subject to such requirement.

- The data retention requirement is redundant with recordkeeping policies and should not be applied to small Covered Entities because it would create a deluge of policies without added benefit.

- Small Covered Entities should not be required to certify compliance with the final rules.

We appreciate the opportunity to offer recommendations to the DFS concerning the Supplemental Proposed Rules and are available to discuss our comments or any of the issues raised by the Supplemental Proposed Rules in greater detail with the DFS or its staff. If the staff has any questions, please do not hesitate to contact Mark Krotoski at (650) 843-7212 or mark.krotoski@morganlewis.com or Charles Horn at 202-739-5951 or charles.horn@morganlewis.com.

Respectfully submitted,

Mark Krotoski, Esq.
Partner, Morgan, Lewis & Bockius LLP

Charles Horn, Esq.
Partner, Morgan, Lewis & Bockius LLP

Morgan Lewis

Appendix A

Mark L. Krotoski
Partner
+1.650.843.7212
mark.krotoski@morganlewis.com

Charles Horn
Partner
+1.202.739.5951
charles.horn@morganlewis.com

November 14, 2016

VIA EMAIL: CyberRegComments@dfs.ny.gov

Maria T. Vullo, Superintendent
New York State Department of Financial Services
One State Street
New York, NY 10004-1511

Dear Superintendent Vullo:

We appreciate the opportunity to comment on the New York State Department of Financial Services' ("DFS's") proposed regulatory framework titled "Cybersecurity Requirements for Financial Services Companies" (the "Proposed Rules").

Morgan, Lewis & Bockius LLP is a global law firm, and many of our clients are licensed with the DFS, including financial institutions, such as banks organized within and outside of the U.S. that do business in New York, and insurance companies. We assist clients in all phases of their cybersecurity needs and issues, including on cybersecurity risk assessments and prevention measures, responding to cybersecurity incidents, and developing cybersecurity policies and programs, and as a result we have a deep familiarity with cybersecurity assessment, prevention and response matters. Because a large number of our clients fall within the scope of the Proposed Rules, we have a substantial interest in the Proposed Rules.

I. Executive Summary

On September 13, 2016, the DFS issued the Proposed Rules, described as "a new first-in-the-nation regulation".[12] The Proposed Rules would require banks, insurers, and other DFS-supervised financial services companies to adhere to stringent cybersecurity requirements mandating firms to test their systems, establish plans to respond to cybersecurity events, and annually certify compliance with the cybersecurity requirements, among other mandates.

---

12 *See* Press Release; Governor Cuomo Announces Proposal Of First-In-The-Nation Cybersecurity Regulation To Protect Consumers and Financial Institutions (Sept. 13, 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf; *see also* New York State Department Of Financial Services Proposed 23 NYCRR 500, Cybersecurity Requirements For Financial Services Companies, *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

We welcome the opportunity to offer our suggestions to enhance the Proposed Rules in this comment letter. In summary, we recommend that the DFS:

- *Introduce a more flexible framework that fosters effective cybersecurity by allowing covered firms to tailor their cyber security efforts to specific cyber risks confronting the firm*. Current government approaches to cybersecurity recognize the need for a firm to tailor its cybersecurity program to its business practices and level of cyber risk by providing principles-based approaches. The DFS should similarly adopt a principles-based approach, which has been demonstrated to be effective. The proposed prescriptive approach will reduce needed flexibility, impose new costly mandatory standards that may be ineffective for Covered Entities (as defined below) and likely will become outdated or obsolete as cybersecurity practices evolve. Additionally, the new prescriptive standards are being imposed in an environment in which Covered Entities must already comply with less-prescriptive standards from other regulators. Instead of imposing new inconsistent standards, DFS should harmonize other cybersecurity standards which will better promote effective cybersecurity with lower costs of compliance.

- *Assure that any reporting requirement be tied to meaningful circumstances connected with the cyber incident and conform with any existing reporting requirements*. The DFS should clarify various aspects of the reporting requirement. For example, the 72-hour reporting timeframe should be extended because it is inconsistent with other regulatory reporting requirements and impracticable in many circumstances. As drafted, the proposed reporting requirement will discourage firms from reporting cyber incidents to law enforcement and also discourage the reporting of cyber threats. In addition, the reporting trigger is too broad and will lead to mandating and over-reporting of insignificant incidents. We contend that the reporting trigger should be based on meaningful cybersecurity incidents.

- *Eliminate the annual compliance certification*. The certification requirement exposes a financial institution's board of directors or senior officer to liability without actually enhancing cybersecurity practices. Because compliance with the Proposed Rules would be required without the certification, the certification requirement does not add value and should be eliminated.

- *Allow a financial institution to rely on a substituted compliance program*. Covered Entities are already subject to cybersecurity oversight by federal and other state regulatory agencies. Where a Covered Entity complies with one cybersecurity regime, it should be permitted to comply with the DFS regime pursuant to a substituted compliance program that is substantively comparable to DFS requirements. By permitting a substituted compliance program, the DFS would reduce the costs of compliance for a Covered Entity, which in turn frees up resources that could be better spent on the Covered Entity's cybersecurity program and incident responses.

- *Eliminate the requirement that a Covered Entity have a Chief Information Security Officer ("CISO")*. The Proposed Rules should not mandate a specific officer-level position to oversee cybersecurity. As a matter of corporate or firm governance, a Covered Entity itself is in the best position to determine how to manage cybersecurity risk.

- *Harmonize its rules and efforts with federal regulatory agencies*. The DFS should strive to reduce inconsistent rules and streamline its regime with other existing or proposed regimes.

- *Expand the proposed exemption for small Covered Entities*. As proposed, the exemption for small Covered Entities still requires small Covered Entities to comply with the majority of the requirements. The DFS should expand the exemption and provide meaningful relief to small Covered Entities.

II. The Proposed Rules Should Allow a More Flexible Framework that Promotes Effective Cybersecurity

In the Proposed Rules, the DFS acknowledges that many firms have already increased their cybersecurity, but that some firms that have not done so should "move swiftly and urgently" to adopt a cybersecurity program.[13] The DFS proposes that all firms subject to the Proposed Rules ("Covered Entities") would be subject to "minimum" cybersecurity standards but cautions against "being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances" without providing evidence that the cost of the Proposed Rules will correspond with their benefits. Instead of adopting a flexible approach based on best practice standards that Covered Entities can adapt to their needs, the DFS has introduced new and specific prescriptive mandates.

It is now widely accepted that cybersecurity policies are most effective when they are tailored to a firm's unique cyber risks and vulnerable information.[14] The DFS should adopt a principles-based approach that Covered Entities can tailor to their business practices. For example, a cybersecurity risk assessment should be tailored to a Covered Entity such that, after the Covered Entity inventories its data, the Covered Entity itself can best determine how to protect the data and how long to retain the data. A cybersecurity program, by its nature, cannot be a one-size fits all program. Rather, the most effective cybersecurity programs take into consideration a host of factors related to the relevant business activities. Federal regulators apply a principles-based approach to cybersecurity, and this approach is more effective because it is flexible, permitting firms to tailor their cybersecurity programs to their unique needs.[15]

---

13 Proposed Rule 500.0.

14 For example, as the Securities and Exchange Commission's ("SEC's") Division of Investment Management's April 2015 Cybersecurity Guidance explains, "[b]ecause funds and advisers are varied in their operations, they should tailor their compliance programs based on the nature and scope of their businesses." Cybersecurity Guidance, SEC Division of Investment Management (Apr. 2015), *available at* https://www.sec.gov/investment/im-guidance-2015-02.pdf. *See also* Mary Jo White's Address to ICI General Meeting (May 16, 2016), *available at* https://www.sec.gov/news/speech/white-speech-keynote-address-ici-052016.html ("While no one can prevent all disruptions from cybersecurity events, you should consider the full range of cybersecurity risks to your funds and consider appropriate tools and procedures to prevent breaches, detect attacks and limit harm.").

15 The Federal Financial Institutions Examination Council, made up of several regulatory agencies, including the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), the National Credit Union Administration ("NCUA"), the Office of the Comptroller of the Currency ("OCC"), and the Consumer Financial Protection Bureau ("CFPB"), as well as state liaison representatives, introduced a cybersecurity assessment tool for banks to use to "help management and directors of financial institutions to understand supervisory expectations, increase awareness of cybersecurity risks, and **assess and mitigate the risks facing their institutions**." FFIEC, Cybersecurity Awareness, available at https://www.ffiec.gov/cybersecurity.htm (emphasis added). *See also* Enhanced Cyber Risk Management Standards, Oct. 19, 2016, to be codified at 12 C.F.R. Parts 30

The need for flexibility becomes all the more important by reason of the wide diversity of Covered Entities in terms of size and nature of business. Covered Entities span the spectrum from insurance companies to banks to financial institutions.[16] Each type of Covered Entity gathers and retains different types of protected data and, accordingly, the cybersecurity systems vary widely amongst these different types of businesses. For example, the cyber risks and type of data and transactions vary among investment companies, insurers, safe deposit companies, and charitable foundations, to consider a few examples of Covered Entities. In addition, Covered Entities vary greatly in their size and sophistication of business activities. The Proposed Rules, however, apply the same standards across all types of Covered Entities, regardless of the nature of business, and to a significant extent, their size.

The current framework introduced by the Proposed Rules does not offer the flexibility needed to adapt over time, while maintaining its effectiveness. The DFS's final rules should identify best practices and standards that Covered Entities can tailor to their unique information systems and cyber risks. As one example, critical infrastructure sectors (16 including the financial services sector[17]) are currently subject to flexible cybersecurity measures pursuant to the National Institute of Standards and Technology ("NIST") framework.[18] The NIST framework was established by an Executive Order with the goal that each critical infrastructure sector would "maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"[19]— calling for a voluntary, flexible framework to achieve this goal. In its *IT Examination Handbook on Information Security*, the FFIEC provides cybersecurity guidance for financial institutions that includes implementing an ongoing security process and ensuring appropriate governance for the security function, among other best practices. However, the FFIEC takes a principles-based approach, recognizing that the steps a financial institution takes should be commensurate with the relevant level of risk.[20]

---

and 364, *available at* https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf. Comments must be received by January 17, 2017.

16 Covered Entities range from banks and trust companies to budget planners, charitable foundations, check cashers, credit unions, domestic representative offices, foreign agencies, foreign bank branches, foreign representative offices, health insurers, accident and related entities, holding companies, investment companies, licensed lenders, life insurance companies, money transmitters, mortgage bankers, mortgage brokers, mortgage loan originators, mortgage loan servicers, New York state regulated corporations, premium finance agencies, private bankers, property and casualty insurance companies, safe deposit companies, sales finance companies, savings banks and savings and loan associations, and service contract providers.

17 Critical infrastructure sectors have been designated as critical because their assets, systems, and networks (whether physical or virtual) are considered so vital to the United States that their destruction or incapacity would have a debilitating effect on the nation's security, economic security, or public health or safety (or any combination thereof). The 16 critical infrastructure sectors include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

18 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology (Feb. 12, 2014).

19 Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2013).

20 IT Examination Handbook on Information Security, Federal Financial Institutions Exam Council (Sept. 2016).

Moreover, the Proposed Rules impose costly measures but may not provide corresponding benefits and, instead, divert resources to support compliance with the Proposed Rules where such resources could be used to support more effective cybersecurity efforts. In adopting the final rules, the DFS should evaluate whether protected data, information systems, and consumers are more secure as a result of this government action. In our experience, flexible standards—even those that are voluntarily adopted—enable firms to focus efforts on certain areas that are specific to the firm's particular needs and will have a greater impact on the prevention of cyber attacks and protection of personally identifiable information. We respectfully encourage the DFS to adopt final rules that enable Covered Entities to approach cybersecurity in a principles-based manner that is tailored to their needs.

III. Any Reporting Requirement Should Be Tied to Meaningful Circumstances Connected with the Cyber Incident and Should Conform with Existing Reporting Requirements

Proposed Rule 500.17 requires Covered Entities to report a "Cybersecurity Event"—defined as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an Information System[21] or information stored on such Information System"[22] —to the DFS within the first 72 hours of a Cybersecurity Event.[23] Based on our extensive experience assisting clients in responding to cyber incidents in the financial services area and many other industries, we believe the proposed reporting requirement is impractical, unrealistic and would discourage reporting cyber incidents to law enforcement and cyber threat sharing information to the government.

We respectfully believe that the DFS should eliminate the reporting requirement since other reporting requirements already apply to Covered Entities. There is little benefit for a new, arbitrary, short reporting requirement. Regulatory agencies should coordinate their efforts in the event of a Cybersecurity Event and facilitate a coordinated approach by relevant regulators and providing the Covered Entity that is the subject of the Cybersecurity Event the opportunity to focus its efforts on resolving the Cybersecurity Event instead of on compliance with myriad reporting requirements.

A. The 72-Hour Reporting Timeframe Is Unrealistic and Impracticable

If the DFS includes a reporting requirement in the final rules, we recommend extending the timeframe to the nature of the incident (as other enforcers have done) rather than impose an arbitrary and unworkable 72-hour standard. The 72-hour reporting window is impracticable and unreasonable. Cyber incidents vary widely in nature and scope. A central issue in any cyber investigation concerns whether relevant data was acquired or exfiltrated. Depending on the nature of the cyber incident, this determination can take weeks or even months to determine. Some sophisticated hackers take steps to cover their tracks and destroy records. For this reason, many

---

21 The Proposed Rules define the term "Information System" to mean "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems." Proposed Rule 500.01(e).

22 Proposed Rule 500.01(d) (Cybersecurity Event Definition) (The term "Cybersecurity Events" is defined as "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".).

23 Proposed Rule 500.17(a) (Notices to Superintendent).

reporting requirements are tied to determinations surrounding the particular cyber incident. For example, the California data breach notification reporting requirement requires notification "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary **to determine the scope of the breach and restore the reasonable integrity of the data system**."[24] Other states have similar standards.

In most cyber incidents, it is not possible to know the scope, nature, and manner of the intrusion for some time. For this reason, notification standards recognize that some time is normally required to determine the scope of the breach. Little may be known about the incident within the first 72 hours of a cyber event, and especially if the event is an unsuccessful attempt.

B. Mandatory Reporting Upon Notifying A Law Enforcement Agency Will Have a Chilling Effect on Providing Information to Law Enforcement

The DFS proposed reporting requirement fails to include a delayed reporting requirement which is widely accepted as necessary to avoid interference with a criminal investigation. Most notification provisions also provide for delayed notification upon the request of law enforcement. For example, the New York State Information Security Breach and Notification Act provides that the notification "may be delayed if a law enforcement agency determines that such notification **impedes a criminal investigation**."[25]

In spite of other New York notification laws, the DFS rule, as proposed, would require notification to the superintendent of "any Cybersecurity Event of which notice is provided to any government or self-regulatory agency."[26] This will discourage reporting cyber incidents to law enforcement. Under this standard, a report to law enforcement in which delayed notification is requested to avoid impeding or interfering with a criminal investigation would be required to be reported to the superintendent. This standard would (1) discourage reports to law enforcement and (2) force a Covered Entity to choose which notification law is being violated, the DFS standard or other applicable reporting requirement that recognizes delayed notification. The DFS should adopt standards that recognize the need for delayed notification and incentivize Covered Entities to work with law enforcement.

C. Mandatory Reporting Upon Notifying the Government About Cyber Threats May Discourage the Sharing of Cyber Threat Information

Additionally, the proposed rule requiring notification of "any" notice that "is provided to any government or self-regulatory agency," may discourage cyber threat sharing that is encouraged to mitigate the breadth of new cyber attacks.[27] Congress recently enacted the Cybersecurity Information Sharing Act of 2015 ("CISA").[28] The U.S. Department of Justice and Department of Homeland Security ("DHS") issued guidance on the sharing of cyber threat

---

24 Cal. Civ. Code § 1798.82(a) (emphasis added), *available at* https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

25 N.Y. Gen. Bus. Law § 899-aa(4) (emphasis added).

26 Proposed Rule 500.17(a)(1).

27 NIST Special Publication (SP) 800-150 (October 2016) *available at* http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf.

28 Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I (2015).

information in June 2016.[29] As required under CISA, DHS has issued further guidance on its website.[30] In order to avoid undermining the sharing of cyber threat information, and these federal standards, the DFS should clarify that cyber threat sharing reports do not fall under the DFS notification requirement.

D. Reporting Should Be Based on Clear, Meaningful Cybersecurity Events

The DFS proposed reporting requirement is also based on a trigger that is too broad with unclear standards. Most other regulatory notification requirements are based on a determination concerning the unauthorized acquisition of information. We encourage the DFS to clarify when reporting is required.

Under the Proposed Rules, the DFS would require a Covered Entity to report upon the "potential unauthorized tampering with, or access to or use of, Nonpublic Information."[31] This is tantamount to requiring notification any time a Covered Entity is attacked, even if there is no acquisition or exfiltration of data. Thus, under the 72-hour notice requirement, a Covered Entity may have to report about an attempt before it can determine whether the attempt potentially tampered with or accessed Nonpublic Information. As already noted, against other notification standards, the proposed DFS notification standard is unrealistically short, arbitrary, unnecessarily broad (it appears to include even unsuccessful attempts), and imprecise on when it is triggered.

To the extent that the final rules include a reporting requirement, we respectfully suggest that the DFS conform these requirements to existing standards that already apply to Covered Entities. There is little benefit to imposing a new, inconsistent reporting standard. The materiality standard contained in the requirement does little to describe the DFS's expectations of when a Covered Entity must report a Cybersecurity Event to the DFS. Further, the DFS broadly defines a Cybersecurity Event to include an *unsuccessful* attempt to gain unauthorized access to a Covered Entity's Information Systems.[32] The Proposed Rules introduce ambiguity as to what, exactly, is required under the reporting requirement. For example, it is unclear whether a non-U.S. Covered Entity based in Japan must report a cybersecurity attack that only impacts its operations in Japan. The DFS should provide precise standards to which non-U.S. Covered Entities regulated by the DFS may adhere. Non-U.S. Covered Entities should not be required to report to the DFS when an attack or breach occurs outside of the U.S. with no impact in the U.S. If the attack or breach has an actual impact in the U.S., only then should the non-U.S. Covered Entity be required to report the event as a Cybersecurity Event to the DFS.

It is also unclear whether the DFS will require Covered Entities to report an unsuccessful cybersecurity attack that would have materially affected normal operations had it been successful. Are unsuccessful attempts, by definition, nonmaterial? If not, the DFS should clarify when it expects a Covered Entity to report an unsuccessful attempt to gain access to its Information

---

29 Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 15, 2016) *available at* https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

30 Department of Homeland Security, U.S. Computer Emergency Readiness Team, Automated Indicator Sharing, *available at* https://www.us-cert.gov/ais.

31 Proposed Rule 500.17(a).

32 Proposed Rule 500.01(d) (Cybersecurity Event Definition) (The term "Cybersecurity Events" is defined as "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".).

Systems. In this regard, large Covered Entities may experience attempted but unsuccessful cybersecurity attacks on a daily basis. Under the Proposed Rules, these events might have to be reported, which could result in large numbers of reports that potentially could dilute the effectiveness of the reporting system, or divert attention away from truly material Cybersecurity Events. We suggest these clarifications to facilitate compliance and a Covered Entity's efforts in the event of a Cybersecurity Event. A Covered Entity's cybersecurity incident response plan incorporates discrete tasks performed by specific personnel at various stages after an event has or is believed to have occurred. Without clear guidance on when reporting to DFS is required, a Covered Entity's cybersecurity incident response plan could, in turn, present reporting ambiguities at a critical point in time. Conversely, DFS could find itself to be a Cybersecurity Event notice repository without the resources to provide meaningful input to a Covered Entity, the public, and other stakeholders when material cybersecurity attacks occur.

Finally, it should be reiterated that notice requirements are growing in number across state and federal statutes or regulations. One of the challenges such requirements present is that they apply different standards for when notice may be given, and under what circumstances. The Proposed Rules add new standards to the regulatory maze of notification requirements. For this reason, we suggest that one federal notification should uniformly apply when a Cybersecurity Event materially impacts protected information located in the U.S.

IV. The Proposed Annual Compliance Certification Should Be Eliminated

Proposed Rule 500.17(b) requires a Covered Entity's board of directors or senior officer to submit to the DFS, on an annual basis, a certification that the Covered Entity is in compliance with the Proposed Rules. We respectfully request that the DFS not adopt this requirement in the final rules. The annual compliance certification potentially exposes the board of directors and senior officer to serious liability if the certification is later found to be inaccurate or inadequate. Not only would there be the risk of direct liability to the DFS, but a finding of an inaccurate certification could potentially expose the financial institution to private liability or collateral action by other state or federal regulatory authorities. In addition, the resources needed to make a certification likely will raise the costs of compliance without increasing security. For example, legal and technical consultants retained to advise a Covered Entity on its certification may divert financial resources from being spent on penetration tests and vulnerability scans, or getting back online in the event of a cybersecurity attack. We question the value a certification made by the board of directors or senior officer would add to a Covered Entity's comprehensive cybersecurity program.

Moreover, we question whether the proposed annual certification requirement would foster effective cybersecurity. The area of cybersecurity is rapidly evolving, and a Covered Entity might be in compliance with the Proposed Rules today, but not tomorrow. The certification potentially may hinder efforts to keep pace with evolving technology and threats. Accordingly, the DFS should eliminate this requirement in the final rules.

In the event that this requirement is retained, the DFS should use an alternative approach to such a certification whereby a Covered Entity's senior officer submits a certification that the Covered Entity has in place cybersecurity policies and procedures that have been *reasonably designed* to comply with the Proposed Rules. Any certification should permit a Covered Entity to explain material noncompliance matters and remediation efforts taken in response to such matters. Such an approach would provide greater insight to the DFS staff on the types of compliance issues that Covered Entities experience and the types of remedial efforts they take to resolve such issues, and could assist the DFS's efforts in this area by providing information about practical approaches Covered Entities in various industries take to address cybersecurity issues as such issues evolve and change.

V. Mandatory CISO Position

The Proposed Rules require Covered Entities to have a CISO. We have not seen a regulation to go so far as to require a CISO, and with good reason.[33] The person responsible for managing cyber risk is a matter of corporate governance, which is generally governed by SEC requirements applicable to public companies. A CISO designation is meaningless unless the person charged with this role has an intimate understanding of a Covered Entity's business practices and technology framework. Moreover, with all of the responsibilities to which a CISO is subject under the Proposed Rules, it is unlikely this role will be easily filled. The Covered Entity itself should be given the flexibility to determine who is best equipped to manage cyber risk and, in some cases, multiple individuals may fill different needs instead of one person overseeing all aspects of cyber risk. [34] For example, a senior manager may be responsible for the cybersecurity policy whereas another senior manager may be responsible for implementing the incident response plan in the event of a cybersecurity incident. The final rules should recognize the importance of compliance with cybersecurity principles instead of micromanaging the way a Covered Entity complies, and it should not matter whether one individual serves as a CISO.

VI. Additional Recommendations

A. The Final Rules Should Allow for Substituted Compliance

The DFS recognizes the "great success" of many Covered Entities in developing cybersecurity programs. Accordingly, the DFS should focus enforcement efforts on Covered Entities that lack effective cybersecurity practices and permit Covered Entities subject to other regulatory efforts to comply with a substituted compliance program that is substantively comparable to DFS requirements.

Most Covered Entities are subject to oversight by multiple regulatory authorities. The Proposed Rules would subject such Covered Entities to multiple regulatory requirements (such as notification requirements) and, in some cases, diverging standards. For instance, New York banking organizations generally are subject to regulation and supervision by one or more federal bank regulatory authorities, which in turn have adopted their own guidance on information security practices, policies, and procedures.[35] Although the federal guidance is, in our view, for the most part not materially at odds with the substantive elements of the Proposed Rules, New York banking organizations will be subject to more extensive prescriptive requirements than the ones that exist at the federal level, and will have to assess their compliance with the Proposed Rules and assure that their cybersecurity programs, policies, and procedures also align with applicable federal guidance on the topic.

---

33 *See, e.g.*, System Safeguards Testing Requirements for Derivatives Clearing Organizations, 81 Fed. Reg. 64,322 (Sept. 19, 2016); *and* System Safeguards Testing Requirements, 81 Fed. Reg. 64,272 (Sept. 19, 2016) (applicable to designated contract markets, swap execution facilities, and swap data repositories).

34 *See*, SEC Office of Compliance Inspections and Examinations, OCIE National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative, Volume IV, Issue 4 at 4-5 (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf (noting that "less than a third of the advisers (30%) [that the SEC examined] have designated a CISO; rather, the advisers often direct their Chief Technology Officer to take on the responsibilities typically performed by a CISO or they have assigned another senior officer (*i.e.*, the Chief Compliance Officer, Chief Executive Officer, or Chief Operating Officer) to liaise with a third-party consultant who is responsible for cybersecurity oversight.").

35 *See, e.g.*, Federal Financial Institutions Examination Council, IT Examination HandBook InfoBase.

To illustrate further the significant overlap the Proposed Rules have with other regulatory efforts, we note that:

- Insurance companies licensed by the DFS would be subject to the Proposed Rules and the HIPAA Security Rule, which requires insurance companies to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting Electronic Protected Health Information ("e-PHI").[36] Specifically, an insurance company subject to the HIPAA Security Rule must:
    - Ensure the confidentiality, integrity, and availability of all e-PHI it creates, receives, maintains, or transmits;
    - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
    - Protect against reasonably anticipated, impermissible uses or disclosures; and
    - Ensure compliance by its workforce.[37]
- Banks that are registered as swap dealers and supervised by the DFS would experience significant inconsistency among regulatory requirements. For example, banks, including foreign banks, that are registered as swap dealers with the U.S. Commodity Futures Trading Commission and members of the National Futures Association ("NFA") must comply with NFA Interpretive Notice 9070, which stipulates that swap dealers must implement a comprehensive written information security program.[38] Although the program must be approved in writing by an executive-level official of the swap dealer, such official is not required to certify the program to NFA or any other regulatory agency, nor is a swap dealer required to notify NFA in the event of a cybersecurity attack. NFA does, however, expect a swap dealer to have an incident response plan that includes the way in which it will address common types of incidents, such as unauthorized access, denial of service, and malicious code.
- Investment advisers registered with the SEC must conduct periodic risk assessments and create a strategy to prevent, detect and respond to cybersecurity threats.[39] Investment advisers must have a cybersecurity program consisting of written policies and procedures, along with training.[40] If such investment advisers are subject to the DFS's oversight, they would be required to comply with incongruous regulatory requirements.

Covered Entities subject to federal and/or state cybersecurity mandates should not be subject to overlapping cybersecurity requirements that would result in increased compliance costs without a significant corresponding increase to cybersecurity effectiveness. The DFS should focus

---

36 *See* 45 C.F.R. § 164.306.

37 *Id.*

38 NFA, Interpretive Notice 9070 (Aug. 20, 2015, effective Mar. 1, 2016), *available at* http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.

39 SEC, Division of Investment Management, Cybersecurity Guidance No. 2015-02 (Apr. 2015). .

40 *Id.*

its efforts on those Covered Entities that are not subject to a multitude of cybersecurity mandates and have not had "great success" in developing effective cybersecurity programs. Further, the DFS should permit a substituted compliance program whereby Covered Entities subject to federal regulatory requirements are not required to also comply with the Proposed Rules. The DFS should deem Covered Entities that comply with federal regulatory requirements to be in conformity with the Proposed Rules after a Covered Entity submits a certification identifying the federal regulator and regulations or other requirements that impose cybersecurity obligations on the Covered Entity. By permitting a substituted compliance program, Covered Entities could use the cost savings to more effectively use their resources to mitigate against cybersecurity attacks and experience greater success in developing cybersecurity programs that would not diminish over time. In turn, their cybersecurity efforts would be enhanced due to greater regulatory clarity and the reduced potential for inconsistent requirements among regulatory regimes.

B. Alternatively, the DFS Should Harmonize Rules with Federal and State Regulators

If the DFS does not provide a substituted compliance program, it should coordinate its cybersecurity efforts with federal and state regulators to prevent inconsistent standards. As DFS is aware, the FRB, OCC, and FDIC recently proposed cybersecurity rules and are still seeking public comment.[41] The DFS should coordinate with the FRB, OCC, and FDIC to streamline regulations applicable to Covered Entities or to confirm that federal regulations provide a satisfactory substituted compliance regime to which Covered Entities could comply instead of the DFS's final rules.

C. DFS Should Expand the Exclusion for "Small Firms"

The limited exemption for "small Covered Entities" under Proposed Rule 500.18 is welcome relief, but we are concerned that the exemption is too narrowly defined to be of real benefit. The DFS should provide more meaningful relief to a greater number of small Covered Entities. The exemption only provides relief from a fraction of the Proposed Rules and still requires a small Covered Entity to create and maintain a policy regarding access privileges, and policies mandating an annual risk assessment, minimum required clauses for third party service provider agreements, and timely document destruction.[42] A small Covered Entity that falls within the scope of the exemption would still be required to notify the DFS of Cybersecurity Events and is subject to its enforcement authority. The relief, then, appears to be quite limited in scope.

Although the requirements to have a CISO, retain an audit trail, and perform penetration testing and vulnerability assessments are costly, and small Covered Entities will certainly be grateful for the cost savings, the limited exemption should provide greater relief from the Proposed Rules by exempting small Covered Entities from Proposed Rules 500.07 (Access Privileges), 500.11 (Third Party Information Security Policy), 500.13 (Limitations on Data Retention), and 500.17 (Notices to Superintendent). A small Covered Entity should not be required to comply with access privileges requirements because, due to a smaller staff, all personnel might have access to all aspects of the small Covered Entity's information systems. This requirement, in practice, would not be useful. Moreover, a small Covered Entity may not have the bargaining power or the funds to retain outside counsel to implement strong cybersecurity provisions in third-party service agreements and, accordingly, should not be subject to such requirement. The data retention

---

41 *See* Enhanced Cyber Risk Management Standards, Oct. 19, 2016, to be codified at 12 C.F.R. Parts 30 and 364, *available at* https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf. Comments must be received by Jan. 17, 2017.

42 Proposed Rule 500.18(a)(3).

requirement is redundant with recordkeeping policies and should not be applied to small Covered Entities because it would create a deluge of policies without added benefit. Small Covered Entities should not be required to report Cybersecurity Events or certify compliance with the final rules. Finally, the DFS's concerns should be where the largest impact on consumers would be in the event of a Cybersecurity Event. A small Covered Entity will presumably have the smallest impact on consumers. The DFS should instead focus its energy and resources on the largest Covered Entities that would have the biggest impact on consumers. In sum, to be meaningful, the exemption should be expanded to encompass a greater number of small Covered Entities.

* * *

For the reasons stated above, we respectfully recommends that the DFS:

- Introduce a more flexible framework that fosters effective cybersecurity.
- Assure that any reporting requirement is tied to meaningful circumstances connected with the cyber incident and conform to any existing reporting requirements.
- Eliminate the annual compliance certification.
- Provide a substituted compliance program.
- Harmonize its rules and efforts with federal regulatory agencies.
- Expand the proposed exemption for small Covered Entities.

We appreciate the opportunity to offer suggestions to the DFS concerning the Proposed Rules and are available to discuss our comments or any of the issues raised by the Proposed Rules in greater detail with the DFS or its staff. If the staff has any questions, please do not hesitate to contact Mark Krotoski at (650) 843-7212 or mark.krotoski@morganlewis.com or Charles Horn at 202-739-5951 or charles.horn@morganlewis.com.

Respectfully submitted,

Mark Krotoski, Esq.
Partner, Morgan, Lewis & Bockius LLP

Charles Horn, Esq.
Partner, Morgan, Lewis & Bockius LLP