INSTITUTE OF INTERNATIONAL BANKERS

299 Park Avenue, 17th Floor
New York, N.Y. 10171
Direct: (646) 213-1149
Facsimile: (212) 421-1119
Main: (212) 421-1611
www.iib.org

RICHARD W. COFFMAN
General Counsel
E-mail: rcoffman@iib.org

Submitted electronically

November 14, 2016

Ms. Cassandra Lentchner
New York State Department of Financial Services
One State Street
New York, NY 10004
CyberRegComments@dfs.ny.gov

Re: Proposed Addition of Part 500 to Title 23 NYCRR
"Cybersecurity Requirements for Financial Services Companies"
(I.D. No. DFS-39-16-00008-P)

Dear Ms. Lentchner,

The Institute of International Bankers ("IIB") appreciates the opportunity to comment on the above-referenced proposed rulemaking (the "Proposal").[1] The IIB's membership is comprised of banking organizations headquartered outside the United States ("foreign banking organizations" or "FBOs") which engage in a variety of banking and other financial activities in the United States and have extensive operations in New York, including New York branches,[2] New York-chartered bank and trust company subsidiaries and New York-licensed nonbank subsidiaries. The Proposal accordingly is of keen concern to our members.

Our members are strongly committed to the robust defense of their operations from cyberattacks and dedicate significant resources to protect and further enhance their information systems, networks and data from all manner of cyber threats and risks. These efforts present significant and ever-changing challenges given the nature of increasing and evolving threats, and it is essential that initiatives to enhance cyber defenses be designed to avoid duplication and achieve the maximum benefits from the additional costs, time and efforts required to be devoted to implementing such measures. Collaborative, risk-based and coordinated actions by the private and public sectors can help enhance the efforts of individual firms beyond what an individual firm or a group of firms can accomplish on their own.

[1] New York State Register, September 28, 2016, pp. 67-69 (the "Notice of the Proposal"). Capitalized terms used in this letter have the meanings ascribed in the Proposal except where otherwise provided or required by the context.

[2] As used in this letter the term "New York branches" refers to New York-licensed branches and agencies of FBOs, collectively.

Our comments in this letter focus in particular on two aspects of the Proposal that raise especially significant concerns specifically for foreign banking organizations:

- The intended scope of the definition of "Covered Entity" as applied to FBOs with respect to their New York-licensed offices.

  For the reasons discussed below in Section I.A, we respectfully request clarification and confirmation that an FBO itself is not a Covered Entity and that the definition, as it relates to FBOs, encompasses only the offices through which FBOs exercise the authority to conduct the business of banking in the State for which they are licensed – *i.e.*, New York branches.

- More generally, the extraterritorial dimensions of applying the proposed requirements.

  As discussed below in Section I.B, in many instances there are close linkages between an FBO and its New York-licensed operations with respect to cybersecurity programs, policies, systems, technology, applications and governance processes. This is especially so with respect to New York branches. We urge the Department to adopt a flexible approach that takes into account these considerations, facilitates compliance and promotes innovation.

  In addition, while FBOs operating in New York are large, global financial services companies in their own right, there is a wide variance in the scale and structure of their New York-licensed operations, ranging from those that are part of a broader U.S. franchise through which the FBO delivers a wide variety of financial services to its clients in the United States, to those that consist of a single branch that is narrowly focused on wholesale banking activities and typically has a small number of employees. These considerations further support adoption of a flexible approach, and we urge the Department to calibrate its cybersecurity requirements accordingly.

In addition to these FBO-specific considerations, we have certain concerns regarding the general structure of the Proposal. Our comments in this regard address, and make recommendations with respect to, the following:

- including in any final cybersecurity regulations express provisions which will ensure a risk-based approach to compliance with the various requirements and avoiding overly-inclusive requirements;

- harmonizing the requirements with existing Federal regulations and cybersecurity frameworks to the maximum extent possible and coordinating closely with Federal authorities in connection with ongoing efforts to enhance cybersecurity protections across the

financial system, including the advanced notice of proposed rulemaking recently proposed by the Federal banking agencies (the "Federal Banking Interagency Cyber ANPR");[3] and

- delaying the effective date and extending the transition periods for any final requirements, as the Proposal goes well beyond current industry practice, and compliance will entail significant additional costs, time and efforts especially with respect to requirements that, as proposed, do not align with existing standards or may not be feasible.

Finally, we provide in the Appendix other comments and recommendations regarding specific provisions of the Proposal not otherwise addressed in the letter. These address concerns which are common to Covered Entities generally and which we highlight to reinforce their significance to our members.

Our comments throughout this letter are intended to strengthen the foundation of the Department's cybersecurity regime, enhance the robustness and effectiveness of Covered Entities' cybersecurity and reinforce the underlying purposes of the Proposal, which the IIB and its members share and to which they are strongly committed. We look forward to continuing to work constructively with the Department on these matters and would welcome the opportunity to discuss further our comments and recommendations.

I. FBO-Specific Concerns and Recommendations

A. Clarifying and Confirming the Scope of "Covered Entity"

We believe there is an unintended ambiguity in the definition of "Covered Entity" as applied to FBOs, and especially with respect to New York branches. An FBO must be licensed by the Department to maintain and operate a New York branch. A license is issued to an FBO and authorizes it to engage in the business of banking in the State through the New York branch in accordance with the requirements of the New York Banking Law (the "Banking Law"). For purposes of determining whether an FBO is a Covered Entity, from this perspective the FBO itself might be understood as the "Person operating under or required to operate under a license" and thus a Covered Entity. This interpretation would result in application of the Proposal's requirements to the global operations of an FBO, a result contrary to the well-established regulatory and supervisory regime applicable to FBOs with New York branches and one that would entail the unwarranted extraterritorial application of New York law.

By comparison, the Department's recently finalized Part 504 regulations prescribing anti-money laundering/economic sanctions transaction monitoring and filtering program requirements

[3] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74315 (Oct. 26, 2016). The ANPR is discussed below in footnote 9.

expressly provide that, as applied to FBOs, the entity subject to the regulation (referred to as the "Bank Regulated Institution") is the New York branch. We see nothing in the Proposal suggesting that the Department intends that the Part 500 cybersecurity requirements be applied differently.

Given the centrality of the definition of "Covered Entity" to the Proposal, and for the avoidance of doubt on this critical, threshold matter, the definition should expressly provide that, as applied to a foreign banking organization per se, it includes only its New York branch and not the FBO as a whole.

We respectfully recommend that this clarification be made by revising the definition of "Covered Entity". In our view, addressing the question indirectly (for example, by including a reference to a branch and agency in the definition of "Person") would be needlessly complex from both a drafting and interpretive perspective. Instead, we believe clarification would be more readily and effectively achieved by adding an explanatory proviso immediately before the period at the end of the proposed definition of "Covered Entity", and we offer the following suggestion, adapted from the definition of "Bank Regulated Institutions" in the Part 504 regulations, for the Department's consideration:

> "provided, however, that in the case of a foreign banking corporation headquartered outside the United States, the term 'Covered Entity' means solely any branch or agency that the foreign banking corporation is licensed pursuant to the New York Banking Law to conduct banking operations in New York and shall not include any branch or agency of the foreign banking corporation located outside New York or the foreign banking corporation itself".

A corollary question is whether New York representative offices fall within the scope of the Covered Entity definition. We respectfully recommend that the Department clarify and confirm that they do not. A representative office license by its very nature is highly restrictive. Further, New York representative offices in general do not maintain their own Information Systems, and they are very limited in terms of not only the scope of their activities, but also the number of personnel. Representative offices do not deal with consumers and do not present any threat to safety and soundness. In our view, imposing the extensive requirements of the Proposal, including a certification requirement, would not serve the purposes of the Proposal as articulated in proposed Part 500 and would result in unwarranted burdens and costs on representative offices. Subjecting representative offices to the Proposal's requirement would create a powerful barrier to entry to the establishment of representative offices in New York and strong incentives to reassess the rationale for maintaining currently-licensed offices. Neither outcome would be beneficial to the State or promote cybersecurity.

B. Extraterritorial Considerations and the Need for Flexibility

We address below our concerns regarding application of the Proposal to the New York operations of foreign banking organizations. We focus on New York branches because it is in this context that the importance of taking into account extraterritorial considerations is especially pronounced since a New York branch is but one part of the global FBO whose head office is outside the United States and whose global operations are overseen by the relevant home country authority, but the same concerns are relevant as well to implementation by FBOs' operations in New York that are conducted through separate legal entities, such as a New York-chartered bank or trust company subsidiary or a New York-licensed nonbank subsidiary, each of which itself is a Covered Entity.

By virtue of their status as offices of much larger foreign banking organizations, the cybersecurity efforts of New York branches in many ways are closely connected to information systems maintained by and information technology developed and provided by the FBO, are supported in certain respects by personnel of the FBO, and operate within parameters established by programs, policies and procedures adopted by the FBO. Similarly, for FBOs with large and complex operations in the United States, the New York branch operates within the large cybersecurity framework established for the FBO's combined U.S. operations.

To ensure the most effective cybersecurity regime in the State, avoid unnecessary duplication and minimize burden and cost, it is essential that any final cybersecurity requirements adopted by the Department reflect and take into account the information security and cybersecurity functional interrelationships that are relevant to New York branches. A plain and unambiguous explanation of the Department's intentions and expectations regarding how the cross-border dimensions of New York branches' operations should be taken into account under the proposed requirements is essential to compliance, including defining the parameters of what is covered by the certification required by Section 500.17(b) (the "Certification of Compliance") and enabling a New York branch to determine the diligence that is necessary to support it.

We identify below specific provisions of the Proposal to which these considerations are especially relevant. We respectfully request clarification of these matters, whether incorporated into any final cybersecurity regulations, discussed in guidance relating to implementation of any such requirements or communicated through some other appropriate means.

1. Cybersecurity Programs and Policies

The cybersecurity programs and policies of a New York branch typically leverage those of the FBO as adapted to take into account its circumstances and local legal requirements. This type of integrated approach to cybersecurity programs and policies strengthens the cybersecurity defenses of New York branches, and it is essential that any final cybersecurity regulations appropriately reflect these considerations.

For example, Section 500.02 refers to aspects of the required cybersecurity program that apply to the Covered Entity's Information Systems, but it does not appear to take into account situations in which a New York branch is connected with and reliant on information systems maintained and operated elsewhere within the FBO group (for example, the FBO itself or a group-level shared services company) outside the New York branch. Clarity on these types of questions is essential to enabling certification to compliance with the regulatory requirement, including identifying the appropriate person who would sign the Certification of Compliance. Similar questions arise with respect to the requirements in Section 500.03 that the Covered Entity's policies address the protection of Nonpublic Information stored on its Information Systems.

2. CISO Requirements

Section 500.04 of the Proposal includes several requirements applicable to a Covered Entity which raise particular compliance challenges for New York branches. For example, Section 500.04(a) would require a New York branch, as a Covered Entity, to "designate a qualified individual to serve as [its] Chief Information Security Officer ("CISO") responsible for overseeing and implementing [its] cybersecurity program and enforcing its cybersecurity policy." For some New York branches, the person who would fill this role and perform these responsibilities may be employed by a U.S. affiliate which is responsible for oversight of the cybersecurity of the FBO's combined U.S. operations, a related service company or by the FBO itself.

We believe flexibility is warranted in all of these instances inasmuch as the purposes of the requirement are equally served so long as the responsible individual possesses the necessary qualifications and authority. Indeed, for those FBOs with diverse U.S. operations such flexibility can strengthen a Covered Entity's cybersecurity efforts by facilitating a coordinated approach across the FBO's U.S. footprint. Flexibility also is appropriate in the case of FBOs which operate in New York principally or exclusively through New York branches. Especially for those whose operations are modest in scale and scope and have a small number of employees, designating a specific individual at the branch is not always feasible, nor should it be necessary so long as an appropriately qualified and authorized individual has been designated.

The Proposal appears to require that the designated individual formally hold the title "Chief Information Security Officer". We do not believe such formal designation is necessary to achieve the purposes of the requirements in Section 500.04 and respectfully request clarification that the designated individual may have the title considered appropriate by the Covered Entity given its organization and structure, so long as the individual is qualified and authorized to discharge the prescribed responsibilities.

To address these considerations, we respectfully recommend that any final cybersecurity regulations provide for designation of an individual to serve the *function* of a CISO and

expressly provide that such individual may be employed by the Covered Entity or one of its Affiliates (which term, as applied to a New York branch, would include the FBO).

Where an individual designated under Section 500.04 (the "Designated Cyber Official") would not be a direct employee of the New York branch and instead be located somewhere in the FBO's group structure outside the New York branch, this arrangement should not trigger treatment of the other entity in the group (whether the FBO itself, a U.S. affiliate or some other related company) as a third party service provider. We believe the provisions of Section 500.04 relating to use of a third party service provider contemplate use of unaffiliated third parties. Extending such treatment to the FBO itself or to members of the FBO group outside the New York branch would result in anomalies such as imposing on the New York branch the obligation to require the FBO to "maintain a cybersecurity program that meets the requirements of this Part" (quoting Section 500.04(a)(3)).

3. Reporting Requirements and Governance Arrangements

Consistent with the foregoing discussion of the CISO requirement, we respectfully request clarification that the Designated Cyber Official would be responsible for any reporting requirement that may be prescribed in final regulations. The Proposal recognizes and provides for the situation in which a Covered Entity may not itself have a board of directors or equivalent governing body.[4] This provision provides helpful flexibility to New York branches, but it does not sufficiently accommodate the recommended role of the Designated Cyber Official. For example, where the Designated Cyber Official is not an employee of the New York branch, it would not make sense to deliver the reports required by Section 500.04(b) to the "Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program." We respectfully recommend instead that the reports be provided to the appropriate Senior Officer(s) of the New York branch.

4. Other Requirements That Implicate Cross-Border Considerations

Similarly, a flexible approach is necessary in applying certain other requirements of the Proposal to the New York operations of foreign banking organizations, including those discussed below, each of which, to varying degrees, entail consideration of cross-border relationships that are essential to those operations. In particular, we believe the suggested clarifications would facilitate compliance with the proposed annual certification requirement.

[4] While not specific to FBOs, we also believe it would be appropriate to provide flexibility in any final cybersecurity regulations so that a Designated Cyber Official could deliver the periodic report to a unit within the Covered Entity's governance structure that is responsible for cybersecurity risk.

a) **Section 500.10. Cybersecurity Personnel and Intelligence.** Similar to our comments regarding the CISO requirement, we respectfully request clarification that compliance by a New York branch or other Covered Entity of an FBO with the requirement of Section 500.10(a)(1) to "employ cybersecurity personnel sufficient to manage the Covered Entity's cybersecurity risk and to perform the core cybersecurity functions" may be based on reasonable reliance by a New York branch or other Covered Entity on personnel employed by a U.S. affiliate, a related service company or the FBO itself.

As a corollary, we further recommend clarification that such reliance would not trigger the requirements of Section 500.10(b) to treat the U.S. affiliate, related service company or the FBO as a third party service provider. With respect to the requirements of Section 500.10(b)(2) and (3), we recommend clarification that these obligations extend only to cybersecurity personnel employed by the New York branch or other Covered Entity of the FBO.

b) **Section 500.16. Incident Response Planning.** We respectfully request clarification that compliance by a New York branch or other Covered Entity of an FBO with any final incident response planning requirements may be based on reasonable reliance on any incident response planning that includes the New York branch or other Covered Entity and is developed and implemented by the FBO or other member of the FBO group, as the case may be.

II. Suggested Improvements to the Structure of the Proposal

A. Clarifying and Confirming the Risk-Based Approach to Cybersecurity Requirements and Avoiding Overly-Inclusive Requirements

The Introduction to the Proposal helpfully states: "This regulation requires each company to assess its specific risk profile and design a program that addresses its risk in a robust fashion." This approach is consistent with the approach taken at the Federal level to enhance cybersecurity, as indicated, for example, by the incorporation of a risked-based approach into the IT Examination Handbook[5] and the Cybersecurity Assessment Tool[6] produced under the auspices of the Federal Financial Institutions Examination Council (the "FFIEC"). A risk-based

[5] FFIEC IT Examination Handbook Infobase (*available at* http://ithandbook.ffiec.gov/it-booklets.aspx).

[6] FFIEC Cybersecurity Assessment Tool, June 2015 (*available at* https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf).

approach also underlies the NIST Framework.[7] Addressing cybersecurity issues from a risk-based perspective is essential to enable Covered Entities the flexibility to prioritize their efforts and deploy their resources in a manner that most effectively enhances their ability to protect themselves against cyber threats.

Further, taking a risk-based approach will facilitate and reinforce the alignment between any final cybersecurity regulations adopted by the Department and standards, guidance and regulatory requirements prescribed at the Federal level to which a Covered Entity is subject. As discussed below, State-Federal alignment and coordination is fundamental to ensuring Covered Entities' cybersecurity defenses are strengthened to the maximum feasible extent.

We are concerned, however, that the risk-based approach does not carry through into many of the proposed requirements, several of which are overly inclusive in their scope and would impede flexible application to Covered Entities' varying circumstances. For example, certain standards in the Proposal would apply to *all* Information Systems and *all* Nonpublic Information irrespective of any risk. In addition, other provisions of the Proposal requiring Covered Entities to put in place certain policies (*e.g.*, application security and third-party information security), controls (*e.g.*, multi-factor authentication and access controls), technologies (*e.g.*, encryption), perform certain tests (*e.g.*, penetration testing) are phrased in extremely broad terms and without any express reference to the application of a risk-based approach. There is a very real risk that such all-inclusive language would result in the application of the standards to systems and data far beyond current practice and what would be practical or necessary to enhance cybersecurity. In addition to creating a tremendous amount of work for Covered Entities – the burden and costs of which should not be underestimated – the provisions as currently drafted would require dedication of resources to protect systems that pose no real risk to customer information or the financial stability of Covered Entities, in addition to adding extra layers of protection where none are needed.

Reliance on a materiality standard to qualify certain requirements is an insufficient substitute for applying a risk-based approach to compliance on a consistent basis throughout any final cybersecurity regulations. We recognize the "filtering" benefits of materiality considerations and believe they should work in tandem with a risk-based approach, but respectfully submit for the following reasons that they should not supplant risk-based considerations:

- Materiality is insufficiently discriminating in its application. It calls for consideration and assessment of the severity of a potential consequence and ignores the equally important

[7] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014 (*available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf).

consideration of its probability. A risk-based approach is based on both considerations and enables a significantly more discriminating and effective basis for identifying and addressing cyber threats and risks.

- Materiality is insufficiently adaptable in its application. It is relatively static compared to a risk-based approach, calling for analysis of a potential consequence without regard to the degree to which a particular cyber threat or risk can be addressed through application of either compensating controls where the prescribed controls don't work (for example, with respect to the use of encryption on legacy or proprietary systems) or newer and better technological solutions (for example, use of tokenization instead of encryption).

- Whereas considerations regarding a Covered Entity's particular circumstances are fundamental to and inherent in a risk-based approach – indeed, it is this aspect that makes a risk-based approach an especially powerful tool in combating cyber threats – a materiality standard is more objective in nature and, as such, less flexible and more susceptible to second guessing.

To address these concerns, and to clarify and reinforce the fundamental importance of a risk-based approach as the Department's guiding principle to enhancing cybersecurity, **we respectfully recommend that any final cybersecurity regulations include a definition of "risk-based approach", and we respectfully suggest the following for the Department's consideration**:

Risk-Based Approach means complying with a provision by (i) carrying out a risk assessment (including, as applicable, an assessment of Information Systems pursuant to Section 500.09) for the purpose of identifying relevant risks and categorizing such risks by severity and probability, (ii) implementing the applicable measure(s) or other superseding or compensating controls, in each case as appropriate in accordance with the level of risk, and (iii) maintaining supportive documentation of steps (i) through (ii).

We further recommend that any final cybersecurity regulations also include an express provision clarifying that a Covered Entity may comply with any requirement by employing this risk-based approach and, by doing so in a manner that satisfies the requirements of the risk-based approach, would be in compliance with such requirement. Moreover, we believe it would be appropriate to provide further that where a Covered Entity applies such a risk-based approach, the time period specified in Section 500.05 and Section 500.11(a)(4) would be interpreted to be the regulatory minimum for the highest risk category, as determined under the risk-based approach, and to apply to lower-risk categories also as determined under the approach. Upon request of the Superintendent or an examiner, the Covered Entity would provide the documentation required by the risk-based approach (or a summary thereof, or both) to demonstrate that appropriate controls have been deployed with respect to an applicable risk.

Our recommended approach would also help to address a concern we have with certain requirements (such as multi-factor authentication, penetration testing and encryption) where the Proposal would lock Covered Entities into implementing specific controls and constrict their ability to adapt to the evolutionary nature of cybersecurity controls and the use of layered controls to achieve similar results. The evolutionary nature of cybersecurity has helped to thwart cybercriminals, and expressly incorporating into any final cybersecurity regulations provisions that recognize and give effect to the variety of Covered Entity's networks, systems and controls, as adapted to their particular circumstances, would strengthen Covered Entities' cyber defenses.

Our concerns with clarifying the centrality of a risk-based approach are heightened by the proposed incorporation of the prescribed requirements into a legally enforceable regulation and to require written certification as to compliance with all of its requirements. Here too a risked-based approach would help allay our concerns. In addition, we respectfully recommended that requirements to "ensure" compliance with particular requirements be removed from any final regulation. Among other concerns, this level of compliance poses very serious challenges to Covered Entities' ability to provide the required certification as it appears to prescribe a standard that contemplates a nearly "zero defects" level of compliance.

B. <u>The Critical Importance of Harmonization and Coordination</u>

IIB members are subject to a broad array of cybersecurity standards and practices prescribed and supervised by multiple Federal and State regulators, as well as by multiple countries. Moreover, these standards and practices continue to evolve to meet the increasing level of cyber threats and risks.[8] The multiplicity and variety of standards creates challenges for financial services firms and can result in redirecting resources from fighting cybersecurity to undertaking assessments necessary for compliance with divergent, and potentially conflicting,

[8] The Federal Banking Interagency Cyber ANPR is a leading example of the continuing evolution of regulatory approaches to cybersecurity. As described in the Federal Register notice: "In response to expanding cyber risks, the agencies are considering establishing enhanced standards for the largest and most interconnected entities under their supervision, as well as for services that these entities received from third parties." We note that many Covered Entities would be subject as well to any such final standards. The ANPR discusses the relationship between existing requirements and the proposed enhanced standards and explains that they "would be integrated into the existing supervisory framework by establishing enhanced supervisory expectations." <u>See</u> 81 Fed. Reg. at 74316. We respectfully request that the Department clarify in connection with any final cybersecurity regulations it might adopt the relationship between such regulations and the type of enhanced standards contemplated by the ANPR.

requirements.[9] In recognition of these challenges, there is a broad international consensus that these multiple efforts should be aligned and harmonized to the greatest extent possible.[10]

Adoption of cybersecurity requirements that in their implementation would be unique to Covered Entities as New York-regulated institutions could have the potential not only to add costs with little benefit to joint efforts by the private and public sectors to enhance the financial services industry's cybersecurity, but also to create potential conflicts that could impede Covered Entities' efforts and potentially place them at a competitive disadvantage, without a compensating improvement in the effectiveness of their cybersecurity.

We strongly urge the Department, in connection with adoption of any final cybersecurity regulations, to harmonize the prescribed requirements with Federal cybersecurity standards and prescribed practices to the greatest extent possible and to articulate its ongoing commitment to continued coordination with its Federal counterparts. Maximizing the alignment between existing and developing Federal standards and requirements to which Covered Entities would be subject under New York law will help Covered Entities focus the deployment of their resources in a manner that takes into account the evolution of cybersecurity practices and permits them to adapt their cybersecurity programs to the inherent risks of their operations.

C. Delaying the Effective Date and Extending the Transition Period

The issues addressed by the Proposal are profoundly important to the safety and soundness of financial institutions and the stability of the financial system. It is imperative to address them in an appropriately deliberate manner in order to avoid unintended consequences and enable Covered Entities to concentrate their cybersecurity efforts in the most effective manner. From this perspective, it is more important to be right than to be first. We believe the proposed January 1, 2017 effective date and 180-day transition period would not provide sufficient time to undertake the careful and diligent assessment of the Proposal and its implications that is critical to making sure that any final regulations most effectively promote

[9] See, e.g., "Regulators Diverge on How Best to Manage Growing Cybersecurity Risks," White & Case LLP Client Alert (November 2016) (*available at* http://www.whitecase.com/publications/alert/regulators-diverge-how-best-manage-growing-cybersecurity-risks.

[10] See, e.g., Treasury and Federal Reserve Support Adoption of The G-7 Fundamental Elements of Cybersecurity for The Financial Sector, October 11, 2016 *(available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0570.aspx); and Baich, Rich, FSSCC Letter to Nakia Grayson Regarding Recommendation to the Commission on Enhancing National Cybersecurity, September 9 2016 (*available at* https://www.fsscc.org/files/galleries/FSSCC_Submission_to_the_Presidential_Commission_on_Enhancing_National_Cybersecurity_Letter_vF.pdf).

Covered Entities' efforts to enhancing their defenses against the very real and increasingly dangerous risks to their operations and the privacy and confidentiality of their customers.

The Proposal presents significant operational and compliance challenges to Covered Entities. It prescribes an extensive array of regulatory requirements, many of which go significantly beyond Covered Entities' current practices, and will put intense pressure on Covered Entities as they determine how best to deploy finite resources, especially at a time when there are many competing compliance demands, including with respect to implementing the new Part 504 regulations. The Notice of the Proposal acknowledges that compliance with the proposed requirements will necessitate increased costs, but we respectfully submit that it understates the impact and consequences for Covered Entities' compliance efforts.[11] Following the issuance of any final regulations, Covered Entities will need to identify gaps between the requirements and their current practices, determine how best to close these gaps, dedicate required budgetary and personnel resources, and undertake the steps necessary to come into compliance. For Covered Entities that are part of an FBO group, this process in many instances will encompass operations and personnel, and implicate governance arrangements, outside the United States.

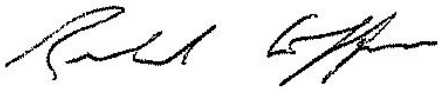
In light of these considerations, we respectfully recommend a delay in the effective date for at least one year and consideration of an extension of the time allowed for the transition period following the effective date. A corresponding adjustment should be made to the date the first Certification of Compliance is required. With respect to the transition period, certain proposed requirements (such as multi-factor authentication, encryption and audit trails) justify a transition period longer than 180 days and perhaps up to two years. Accordingly, we respectfully recommend that the transition period be extended (i) for one year, if the effective date is extended for one year, and (ii) for two years, if the effective date is not extended. Finally, any final cybersecurity regulations should address the timing of the application of their requirements to entities which become Covered Entities after the effective date.

* * *

[11] The Notice of the Proposal states that the proposed rule will impose "some costs" on Covered Entities' operations, which will be offset "to varying degrees" through avoidance or mitigation of cyber attacks that, but for compliance with the rules, "might otherwise have caused financial and other losses." The Notice provides no further explanation of the bases for these conclusions and does not explain the methodology for estimating the Proposal's costs. We strongly agree that enhancing cybersecurity defenses is essential and will benefit both individual firms and the financial system in general, but we would respectfully request the Department to give closer attention to the magnitude of the changes to Covered Entities' current practices, and the resulting increase in the demands on their resources and the costs of compliance, contemplated by the Proposal.

We appreciate your consideration of our comments and recommendations and would welcome the opportunity to discuss them further with you and your colleagues. In the meantime, please contact the undersigned or Paul Begey (pbegey@iib.org; 646-213-1146) at the IIB if you have any questions.

Sincerely,



Richard Coffman
General Counsel

APPENDIX

OTHER COMMENTS AND RECOMMENDATIONS ON SPECIFIC PROVISIONS OF THE PROPOSED REGULATIONS

As discussed in the letter to which this Appendix is attached, the comments provided below address concerns which are common to Covered Entities generally and which we highlight to reinforce their significance to our members. Concerns regarding application of certain of the requirements specifically to foreign banking organizations, as well as our recommendations for improving the overall structure of the regulation (such as expressly incorporating a risk-based approach into each Section as appropriate), are addressed in the letter.

Section 500.01. Definitions.

Covered Entity

We respectfully request clarification in any final cybersecurity regulations of the status as a Covered Entity, and the applicability of such requirements to its activities, of a legal entity that (i) is a subsidiary of another legal entity that itself is not a Covered Entity, but that (ii) would appear to fall within the terms of the definition of Covered Entity because a portion of its business in New York involves activities which trigger the Department's licensing requirements (such as insurance or mortgage banking activities undertaken in connection with acting as a securities broker-dealer). In the extreme case, such an entity would be the only entity within a financial services group that would be subject to the requirements as a Covered Entity, but the same questions arise where there may be one or more other Covered Entities within the group and where the entity engages solely in activities requiring a license (such as insurance agency activities) rather than merely as an adjunct to other activities.

Key concerns regarding such entities include the following:

- the prospect that treatment of such an entity as a Covered Entity, and imposition of the various prescribed requirements, would impose disproportionate compliance burdens and costs on the entity (this concern would be magnified where the entity otherwise is subject to cybersecurity standards/requirements prescribed by a Federal regulatory authority); and

- the risk that imposing such requirements would, as a practical matter, entail their "exportation" to other members of the group that are not otherwise subject to the requirements (this concern would be especially pronounced where the entity would be reliant on or interconnected with other members of the group with respect to, for example, its information systems) such that the other members of the group would become *de facto* Covered Entities.

To address these concerns, we believe it would be appropriate to provide a mechanism that would enable a Covered Entity to discuss its situation with the Department and work out an arrangement with the Department that is reasonable under the circumstances, including, where appropriate, a full or tailored/partial exemption from the requirements. We believe it would be appropriate to review these situations from a risk-based perspective and calibrate the regulatory response accordingly. These provisions would be distinct from the limited exemption available under proposed Section 500.18, which would subject a Covered Entity to the most significant requirements of the Proposal and, as such, would not be sufficient to accommodate the situations contemplated by our recommendation.

Cybersecurity Event

The definition of a Cybersecurity Event is very broad in that it would include *all* successful and unsuccessful events. So broadly defined, such events can number in the several thousand per day for some of the larger institutions. As discussed below, the breadth of the definition poses very real and difficult implications for compliance, and in particular with the proposed notice requirements of Section 500.17(a).

To address these concerns, we respectfully recommend limiting the definition of a Cybersecurity Event to successful acts that have a substantial likelihood of having a material impact on a Covered Entity.

Information Systems

The definition of an Information System also is overly broad, especially the inclusion of "any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems", which would appear to bring into scope many other systems regardless of their relevance to cybersecurity or whether they are more traditionally considered as information systems. Given the centrality of the definition to the substantive requirements of the proposed regulations, its extensive breadth would pose very substantial compliance challenges, including with respect to the Certification of Compliance, especially if any final regulations were adopted on the timeline contemplated by the Proposal.

To address these concerns, and to promote consistency in applicable standards, we respectfully recommend adoption of an approach that more closely aligns with the FFIEC's definition and incorporates a risk-based approach that would allow Covered Entities flexibility in determining what additional systems protections should be applied and to what extent.

Nonpublic Information

Here too, the proposed definition is overly broad in that it encompasses "all electronic information that is not Publicly Available Information" and meets the other prescribed criteria. As this definition also is central to operationalizing the substantive requirements of the proposed regulations, we are concerned that such overbreadth would impede truly effective risk-based implementation. In addition, taking into account the considerations discussed below regarding the definition of "Publicly Available Information", we are concerned that as a practical matter Covered Entities would default to treating virtually all information as Nonpublic Information, regardless of whether, with respect to business related information, disclosure would have any material adverse impact to the business, operations or security of the Covered Entity. Such an unintended consequence would significantly compound Covered Entities' compliance challenges, including providing the Certification of Compliance, without enhancing their cybersecurity. There is also the risk that during examinations certain information would be required to be treated one way pursuant to Part 500, but not all of the same information would be required to be treated the same way by Federal examiners.

To address these concerns, we respectfully recommend the following bifurcation of the definition as it relates to non-health-related information:

- **Information regarding individuals** would track the definition of "nonpublic personal information" under the Gramm-Leach-Bliley Act and thereby enable Covered Entities to utilize the policies, processes and system already in place.

- **Business-related information** would be identified through a risk-based approach based on information that is considered confidential, coupled with something like the proposed "material adverse impact" standard.

Publicly Available Information

As discussed above, the definition of Publicly Available Information is used in the definition of Nonpublic Information to bring into scope all information that is not otherwise publicly available. The definition lists several types of information made available to the general public including "federal, state or local government records; widely distributed media; or disclosures required to be made by federal, state or local law." These descriptors make clear what is intended to be publicly available information. However, the definition also requires Covered Entities to take steps to determine, among other things, "[w]hether an individual can direct that the information not be made available to the general public *and, if so, that such individual has not done so*" (emphasis added).

We are concerned that these requirements would pose practical obstacles to compliance and would result in Covered Entities defaulting to treatment of information as Nonpublic

Information. To address this concern, we respectfully recommend that the definition be revised to provide that Publicly Available Information is any information that is not within the definition of "Nonpublic Information," modified as we suggest above.

Section 500.03. Cybersecurity Policy.

The Proposal would appear to suggest that there should be a single, unified cybersecurity policy that covers fourteen different areas, whereas many of the areas listed frequently are addressed in separate polices, frameworks, standards or plans that go beyond just cybersecurity. For example, business continuity and disaster recovery plans, deal with various types of threats (*e.g.*, natural disasters, terrorist attacks, and utility outages), with a cyber threat being only one of any number of potential threats addressed in a business continuity plan.

Individuals who work on these business continuity policies are experts in these areas and consider the occurrence of multiple threats at once – for example, the concurrence of a cyber threat and a power outage. Allowing a firm to comply with this requirement through referencing/cataloging existing policies would avoid duplication, and any potential issues because of a conflict between a cybersecurity policy and any separate policies. We respectfully request clarification of the Department's expectations in this regard in connection with adoption of any final cybersecurity regulations. For example, provisions could be added at the end of Section 500.03(a) explaining that the required cybersecurity policy may include one or more written documents, whether titled as policies, frameworks, standards or some other term, that together address the 14 prescribed areas.

Section 500.04. Chief Information Security Officer.

In addition to the discussion above in Section I.B.2 and .3, we respectfully recommend the following:

- **Annual Reporting** – The report should be required in general only annually, as work required to produce and validate the report will be considerable. A bi-annual reporting period would have the unintended consequence of requiring Covered Entities to be in a near constant state of preparing the reports, and divert resources from other cybersecurity activities.

- **Level of Detail** – Given the governance level at which this report is to be provided, and considering the technical nature of some of the reporting items (for example, paragraph 500.04(b)(5) requires the report to address "proposed steps to remediate any inadequacies identified"), the reporting requirement should be qualified by a term, such as "reasonable specificity."

- **Confidentiality** – Given their content, it should be explicitly stated that these reports, when and if delivered to the Superintendent, are considered "confidential supervisory information" subject to Banking Law Section 36.10.

Section 500.05. Penetration Testing and Vulnerability Assessments.

Proposed Section 500.5 requires penetration testing of all Information Systems at least annually and vulnerability assessments of Information Systems at least quarterly. While penetration testing and vulnerability assessments are valuable tools, there are other tools that can be used to achieve the same objectives with similar effectiveness. For example, red teaming can be used to simultaneously assess vulnerabilities of networks and systems and conduct penetration testing. Many firms place scanners on their networks to assess vulnerabilities on an on-going basis. Penetration testing is only as good as the practitioner conducting the test, and tools used to conduct vulnerability assessments are in some ways limited (for example, they require software updates and are able to expose only known vulnerabilities). This is an area that continues to evolve and where firms welcome new technologies and methods.

In light of these considerations, we respectfully recommend that this requirement allow for substantive equivalents to penetration testing and vulnerability assessments, referencing penetration testing and vulnerability as examples of the type of assessments required.

Section 500.06. Audit Trails.

While many of the requirements under proposed Section 500.06 are currently performed by financial services firms, the requirement that Covered Entities "track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a Cybersecurity Event" goes well beyond industry practice. In addition, the need to maintain these audit trails for six years deviates significantly from the current industry standard of maintaining logs for one year, and will require significant resources given increased storage requirements and the need to index the records.

Moreover, the requirement to have a system that allows for the "complete and accurate reconstruction of all financial transactions and accounting" generally is not currently feasible. In addition, it is unclear (i) whether the requirement extends to data on all systems on which financial transactions may be carried out, including systems where a Covered Entity may be only one user; and (ii) whether the reference to "accounting" means an accounting audit trail. More generally, and apart from these considerations, the broad definition of Information System would significantly increase Covered Entity's compliance costs and burdens without necessarily enhancing their cybersecurity.

Incorporating a risk-based approach into any final prescribed requirements, coupled with extending the effective date and transitional periods, would significantly diminish the foregoing concerns.

Section 500. 07. Access Privileges

We understand that what is being required in this section in terms of limiting access privileges in many instances is already being done. However, given the broad definition of Information Systems, the requirements could apply to systems heretofore not considered subject to such limits, thereby increasing compliance costs and burdens.

Adopting a risk-based approach to these requirements, coupled with extending the effective date and transitional periods, would significantly diminish these concerns.

Section 500. 11. Third Party Information Security Policy

A risk-based approach should be permitted with respect to vendor assessments, as is currently the practice today. Given the hundreds, if not thousands of vendors a typical firm may have, a risk-based approach will best ensure that resources are focused on vendors that pose the greatest risk. For example, it is not feasible in many instances to conduct a periodic, annual assessment of all vendors as would be required by Section 500.11(a)(4). We accordingly respectfully request that any final cybersecurity regulations limit such assessments to critical third parties, where criticality is determined under a risk-based approach.

Moreover, a risk-based approach would take into account the reality that certain large vendors exercise a degree of market power that, as a practical matter, would prevent a Covered Entity from effectively seeking to obtain from the vendor many of the "preferred provisions" listed in Section 500.11(b), such as use of multi-factor authentication and encryption and the right of the Covered Entity or its agent to perform cybersecurity audits of the vendor.

We would also make the additional following recommendations with respect to this Section:

- A Covered Entity should not necessarily and in all circumstances have to treat a parent or related entity as a third party for purposes of this section.

- A third party's need to notify a Covered Entity under Section 500.11(b)(3) of a Cybersecurity Event that effects the third party should be limited to instances where there is a potential for that Cybersecurity Event to effect the Covered Entity.

- The third party's need to provide identity protection services under Section 500.11(b)(4) should be limited to instances where an individual is involved.

Section 500.12. Multi-Factor Authentication.

Section 500.12(b) of the Proposal requires multi-factor authentication for "privileged access to database servers that allow access to Nonpublic Information." Applied to an internal network, this requirement would result in use of multi-factor authentication to access the network and then used to access the database. The multi-factor authentication requirement would apply regardless of any risk related to accessing the system and data, and regardless of other and potentially better controls that may be in place. Adoption of a risk-based approach, which would take into account the strength of a Covered Entity's internal controls would significantly diminish this concern.

In addition, we respectfully recommend that any final cybersecurity regulation allow for other authentication methods based on the judgment of the firm. Multi-factor authentication is not impervious to cyberattacks, and although the Proposal requires risk-based authentication for accessing Nonpublic Information through web applications, given the evolution of cyberthreats, no method is impervious to intrusions over any length of time. Therefore, we respectfully recommend allowing flexibility in meeting this requirement through the use of "effective controls" using multi-factor authentication and risk-based authentication as examples. This will allow firms to put in place alternative methods and new authentication controls as they are developed.

Regarding the application of multi-factor authentication with respect to accessing web applications as provided in Section 500.12(c) and (d), we respectfully recommend that the focus of these requirements be directed at accessing external, internet-facing applications.

Section 500.13. Limitations on Data Retention.

As drafted, the Proposal's data retention standard would require the destruction of Nonpublic Information "that is no longer necessary for the provision of the products or services for which such information was provided to the Covered Entity." This standard does not take into account forms required for the provision of services, but may be necessary at a later date to demonstrate customer authorization, or information necessary for a firm to defend itself if an action is brought against it.

To address these concerns, we respectfully recommend than any final cybersecurity regulation rely on a firm's data retention policy and the justification for the retention of specific non-public information to satisfy this requirement.

Section 500.14. Training and Monitoring

Paragraph 500.14(a)(2) requires "all personnel to attend regular cybersecurity awareness training sessions." We respectfully recommend flexibility be provide in meeting this standard,

as firms may employ other training techniques, such as online modules and written materials to train personnel.

Section 500.15. Encryption of Nonpublic Information.

Section 500.15 of the Proposal calls for the encryption of Nonpublic Information, stating "each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest." Given the very broad definition of what constitutes Nonpublic Information, this requirement goes far beyond industry practice with respect to the use of encryption – where encryption is normally employed on a risk-based standard – and would create massive technical and financial challenges. Although the Proposal would allow the use of compensating controls for Nonpublic Information in transit and at rest for either up to one year and or to five years, respectively, in some cases it may be impossible to put in place encryption for data at rest (*e.g.*, with respect to legacy systems or comingled data). With respect to data in transit, in some instances encryption either would be of little practical value (for example, (i) for internal data at rest, where imposing encryption would not stop the relevant data from being available internally in unencrypted form as the information needs to be decrypted to be used by applications; and (ii) for data internally in transmit, where encryption would impede surveillance of internal network traffic to detect intruders) or would thwart Covered Entities' progression to use of alternative, and potentially more effective methods (*e.g.*, tokenization).

The technical challenges presented by the proposed encryption requirement include:

- the need for hardware and software upgrades to address the increased processing required to encrypt and decrypt vast amounts of data;

- a reduction in transaction speed, as result of latency issues, which can be critical for certain applications and potentially create a competitive disadvantage for Covered Entities;

- conflicts with (if not the inability to use) legacy systems that have been integrated into some Covered Entities' operations; and

- potential negative impacts on the effectiveness of other cyber security controls like Data Loss Prevention solutions.

The adoption of a risk-based approach (as recommended) to encryption (as is currently permitted under applicable Federal standards) would allow for compensating or superseding controls in place of encryption and would significantly diminish these concerns.

Section 500.17. Notices to Superintendent and the Certification of Compliance (Attachment A to the Proposal).

Section 500.17(a) Notices. As discussed above, it is expected that the definition of Cybersecurity Event would result in a massive number of notifications to the Superintendent, thereby raising questions regarding their utility. In addition, we anticipate the requirement would severely stretch the Department's ability to absorb so many filings and meaningfully analyze their contents. These concerns are magnified by the vague requirement that a notice be provided with respect to any Cybersecurity Event that "affects" Nonpublic Information (which, as discussed above, is itself very broad in its scope).

Revising the definitions of Cybersecurity Event and Nonpublic Information as recommended above would help diminish the compliance burden of the proposed notice requirement and improve the prospects that the notice would produce practical benefits. However, it is unclear from the Proposal what exactly Covered Entities are required to report in their notices and how they should submit the reports (as to this latter consideration, we understand the Department would provide a secure portal for submission of the notices). Understanding the content of the notice is essential to assessing the practicality of the proposed 72-hour submission requirement, which, in any event, we respectfully recommend be revised to provide, at a minimum, that the filing would be required no sooner than 72 hours after the Covered Entity has confirmed the Cybersecurity Event that is being reported. These same considerations apply equally to notices of "material risk of imminent harm" required under Section 500.17(b)(2).

More generally, we believe the provisions of proposed Section 500.17(a) require significant reconsideration, including whether 72 hours, however measured, is a reasonable period of time to enable submission of practically useful information. Regarding the notice requirement more generally, we respectfully recommend the following:

- An exception should be provided to permit delayed notification where law enforcement has requested that a Covered Entity not disclose information regarding a Cybersecurity Event.

- Given their content, it should be explicitly stated that any notice submitted pursuant to Section 500.17 shall be considered "confidential supervisory information" subject to Banking Law Section 36.10. This recommendation applies equally to the Certification of Compliance required under Section 500.17(b).

Section 500.17(b) Certification of Compliance. The Certification of Compliance clearly is modeled on the certification required under the Department's new Part 504 regulations. Like that certification, the proposed Part 500 certification contemplates reliance on internal reports, sub-certifications and opinions from relevant personnel. Bank Regulated Entities (as that term is defined in Part 504) are experiencing significant challenges in putting in place the

policies, processes and protocols to support that certification, and we anticipate that the challenges will be no less daunting under Part 500. As discussed in the letter to which this Appendix is attached, these considerations argue strongly in support of delaying the effective date and extending the transition period of any final cybersecurity regulations.

Regarding the proposed terms of the Certification of Compliance set forth in Attachment A to the Proposal, we note first that the provisions of paragraph (3) are blank. Also, it is unclear what is contemplated by the statement that the individual signing the Certification has undertaken diligence "as necessary", an ambiguity that raises the prospect of "second guessing" the sufficiency of the diligence a Covered Entity undertakes. Further, the Certification would be made without qualification save for being made to "the best of the [individual signatory's] knowledge." Read in conjunction with the undertaking that the individual has conducted diligence "as necessary", it would appear that the qualification as to "best knowledge" would provide minimal protection in the event the certification were called into question. This concern regarding the essentially blanket nature of the certification would be diminished to the extent a risk-based approach were consistently and expressly incorporated into the underlying substantive requirements as to which the individual is certifying compliance. However, the certification nevertheless would still be made on an essentially unqualified basis.

Regarding the other provisions of Section 500.17(b), we respectfully request clarification of the following:

- Where a Covered Entity has "identified areas, systems, or processes that require material improvement, updating or redesign" (quoting Section 500.17(b)(1)), can it provide a "clean" Certification of Compliance? This concern could be mitigated by, for example, incorporating into the Certification an exception that would address such instances.

- Regarding notices of "imminent harm" required under Section 500.17(b)(2), what is a Covered Entity required to include and how should it include these "in its annual report" (*i.e.*, the Certificate of Compliance)? The form of the Certification provided in Attachment A to the Proposal does not address these matters.