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

February 17, 2017

Robert deV. Frierson
Secretary
Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
regs.comments@federalreserve.gov
(Docket No. R-1550, RIN 7100-AE 61)

Legislative and Regulatory Activities
Division
Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218, mail stop 9W-11
Washington, DC 20219
regs.comments@occ.treas.gov
(Docket ID OCC-2016-0016)

Robert E. Feldman
Executive Secretary
Attn: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
comments@fdic.gov
(RIN 3064-AE45)

Re: Enhanced Cyber Risk Management Standards

Ladies and Gentlemen:

The Institute of International Bankers ("IIB") appreciates the opportunity to comment on the advance notice of proposed rulemaking referenced above.[1] The IIB's members are 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. Our members are strongly committed to the robust defense of their operations and protection of customer information from cyberattacks, and they dedicate significant resources to reinforce their information systems, networks and data from all manner of cyber threats and risks.

[1] 81 Fed. Reg. 74315 (October 26, 2016) (the "Proposal"). Capitalized terms used in this letter have the meanings ascribed in the Proposal, except as otherwise indicated or required by the context.

Protecting and reinforcing the cybersecurity of financial institutions is fundamental to their operational resilience and essential to strengthening the stability of the financial system. The challenges in this area are daunting and constantly evolving, and the issues presented are complex and not well-suited to overly prescriptive solutions. We appreciate the Agencies' approach to developing enhanced cyber risk management standards by means of a joint ANPR. This process permits the deliberate and thoughtful consideration of how best to build upon the many advances that have been made in the area to date and is more likely, ultimately, to avoid unintended, and potentially counterproductive, consequences that can result from a "rush-to-judgement" or "first-to-the-finish" perspective on rulemaking. As well, we applaud the coordinated, inter-agency approach taken in addressing these very significant cybersecurity matters, and we look forward to continuing to work with the Agencies on this initiative.

The IIB is a co-signatory of a separate letter on the Proposal spearheaded by the Securities Industry and Financial Markets Association (the "SIFMA Letter"). We are submitting this letter on our own behalf to address certain aspects of the Proposal as they apply specifically to FBOs.

As an initial matter, we support determining the scope of application of the enhanced standards based on an FBO's combined U.S. operations ("CUSO") and applying the standards to those operations on an enterprise-wide basis.[2] Regarding federal branches and agencies, it would be helpful to clarify that any OCC-prescribed standards would apply only to those which themselves meet the prescribed threshold.[3]

Regarding other FBO-specific aspects of the Proposal, the following matters should be clarified:

---

[2] The proposed $50 billion total consolidated asset threshold for designating those entities that would be subject to the standards ("Covered Entities") aligns with the threshold prescribed in Section 165 of the Dodd-Frank Act for the application of the enhanced prudential standards prescribed thereunder, and applying this threshold to FBOs based on a CUSO-only basis would be consistent with the approach taken by the Board in applying certain of those standards to FBOs. As discussed in the SIFMA Letter, size should not be the only determinative factor in delineating the scope of Covered Entities. To the extent the statutory threshold under Section 165 provides a reference point for the determination of Covered Entities as the Agencies proceed with their cyber risk rulemaking, appropriate revisions should be made to reflect any modifications to that threshold.

[3] Such clarification would make the approach taken to federal branches and agencies in any future rulemaking on this subject consistent with the approach taken to application of the heightened risk governance standards prescribed in Appendix D to Part 30 of the OCC's regulations, which we believe is what is intended.

- CUSO Governance

  The Proposal notes the close connection between the contemplated cyber risk governance arrangements and the larger risk management framework applicable to U.S. bank holding companies under the Board's Regulation YY.[4] With respect to Covered Entities that are comprised by the combined U.S. operations of FBOs it is evident that a similarly close connection is intended with the CUSO risk management framework set forth in Section 252.155 of Regulation YY.[5] However, it is unclear how the responsibilities assigned to the "board of directors" under the Proposal are intended to be exercised in the circumstances of those FBOs whose combined U.S. operations include a U.S. branch or agency, and especially those that are not required under Regulation YY to establish a U.S. intermediate holding company. We would welcome the opportunity to discuss these considerations further as the rulemaking process progresses.

- Internal and External Dependency Management in the FBO Context

  Regarding the application of the proposed "internal dependency" and "external dependency" standards to an in-scope U.S. branch or agency, the question arises how the FBO, as the global legal entity of which the U.S. branch/agency is a part, should be treated. The closely related question is the extent to which the enhanced cyber risk management standards would apply extraterritorially, thereby raising questions regarding potential conflicts or inconsistencies between the U.S. standards and standards or requirements to which the FBO is subject under the applicable law of its home country or other host countries. We believe the relationship between a U.S. branch/agency and the FBO would be better characterized as an external dependency for these purposes. In addition, and to further appropriately limit the potential extraterritorial application of the U.S. standards, we believe that an FBO should not be characterized as a third-party service provider to its combined U.S. operations. We also would welcome the opportunity to discuss these considerations further as the rulemaking process progresses.

Although the question is not FBO-specific, the Agencies solicit comments on three possible regulatory approaches to establishing enhanced cyber risk management standards. Among these three approaches, and emphasizing that any approach must be appropriately risk-based, we believe a combination of a regulatory requirement to maintain a risk management framework for cyber risks along with a policy statement or guidance that describes minimum expectations for the framework would most effectively achieve the intended purposes of adopting an approach whose standards are clear, adaptable to ever-evolving cyber challenges,

[4] See 81 Fed. Reg. at 74321, footnote 17.

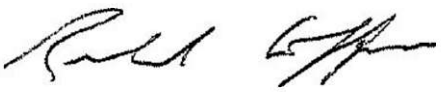
[5] See 81 Fed. Reg at 74320, footnote 15.

and achievable by means that appropriately balance effectiveness and robustness against potential costs and other burdens associated with implementation.

* * *

We appreciate your consideration of our comments. Please contact the undersigned if we can be of further assistance.

Sincerely,



Richard Coffman
General Counsel