Timothy D. Adams
President and CEO

June 9, 2017

Mr. Svein Andresen
Secretary General
Financial Stability Board
Bank for International Settlements
CH-4002 Basel
Switzerland

Re: IIF support for FSB focus on cyber risks and stock-take of cyber security regulation

Dear Svein:

The Institute of International Finance (IIF) welcomes the Financial Stability Board's ("FSB") effort to better understand cyber risks, including a stock-take of existing cyber security regulation, as a basis for developing best practices in the medium-term.[1]

The IIF and its members are committed to working closely with the public sector on issues around cyber security, and particularly to address risks with implications for financial stability. We value the opportunity to provide input to your important initiative.

In particular, the IIF would like to emphasize our concern that increasing fragmentation of regulatory approaches by governments is presenting serious challenges to the ability of financial institutions to effectively address cyber risk. As regulatory attention to cyber risks increases, we have observed an increasing number of proprietary national approaches:

- In the U.S., for example, various financial regulators have issued multiple different proposals, including the FFIEC's 'Cybersecurity Assessment Tool', the OCC, FDIC, and FRB's 'Enhanced Cyber Risk Management Standards', the CFTC's 'Enhanced Rules on Cybersecurity' and 'Final Rules on System Safeguard Testing', and state-level cyber security regulations issued or proposed by New York, Colorado, and California; none were harmonized with each other or existing frameworks and approaches;

- In Asia, while government and regulatory agencies maintained open lines of communication during their rule-making processes, regulatory harmonization on a large scale remains difficult, and we have observed the proliferation of unique, non-standardized rules either proposed or issued by agencies of China, Hong Kong, Singapore, India, and Malaysia;

[1] Mark Carney, "Building the Infrastructure to Realise FinTech's Promise," speech at the International FinTech Conference 2017, London, April 12, 2017.

- Regulatory activity in Europe has also increased, and despite the presence of established regional governing structures such as the European Commission and European Central Bank, individual member states within the region such as the U.K., France, and The Netherlands continue to move forward with their own distinct regulatory efforts.

Especially for firms that operate in multiple jurisdictions, this fragmentation is adding complexity and diverting resources away from security-related activities toward compliance requirements. Disparate regulations or guidelines with differing standards and conflicting expectations may also result in confusion for financial institutions operating in multiple regulatory environments. Additionally, cyber security is a global issue that rarely happens within national borders or is constrained to one economic sector, therefore it should be avoided that weak-links form in jurisdictions or industries, including new entrants, where lower standards might apply, posing risks to others in the global financial ecosystem.

We hope that these issues will be raised by the FSB as part of your stocktaking on cyber security regulation. By underscoring the risks around regulatory fragmentation, the FSB could help enable firms of all sizes to greater meet their compliance requirements, security needs, and facilitate improved coordination of cybersecurity supervisors. Increased coordination by international standard setters to promote common standards and approaches could both address the regulatory fragmentation and further support financial stability.

It should be noted that there are already in existence excellent international resources for regulators including the G7's non-binding "Fundamental Elements of Cybersecurity for the Financial Sector"[2], designed to help bolster the overall cyber security and resiliency of the international financial system. There are already examples, such as the U.S. NIST Cybersecurity framework, where these principles have been embraced and which are supported by many financial institutions. Similarly, there are also the CPMI-IOSCO cyber resilience guidelines, which were the first cyber guidelines issued by the international financial sector standards-setting bodies.[3]

The industry would welcome the opportunity to collaborate with the FSB and the global regulatory community to offer lessons-learned and expertise on effective cyber practices and assessments. This could include increased public-private collaboration, given the shared interest among both the public sector and industry in finding solutions, sharing information and building resilience across the financial system.

The IIF is encouraged by the focus of the FSB on these important topics, given the new risks arising from outside the regulated financial industry; the sharp increase in the number, scope and sophistication of recent cyber attacks; and, the implication to protecting financial stability across the system, and the Institute stands ready to contribute to your efforts in whatever ways would be appropriate.

---

[2] G7, Oct. 11, 2016. http://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf

[3] CPMI-IOSCO, June 2016, http://www.bis.org/cpmi/publ/d146.pdf

The IIF welcomes continued dialogue on this important matter. If you have any questions on the issues raised in this letter, please contact myself or Martin Boer, IIF's Director of Regulatory Affairs (mboer@iif.com).

Sincerely,

cc: Mr. Rupert Thorne, Deputy to the Secretary General, Financial Stability Board
Ms. Susan Nash, Member of the FSB Secretariat
Ms. Grace Sone, Member of FSB Secretariat
Mr. Fernando Restoy, Chairman, Financial Stability Institute