Written Statement of Kenneth E. Bentsen, Jr., President and CEO, SIFMA

before the Committee on Financial Services

Subcommittee on Financial Institutions and Consumer Credit

U.S. House of Representatives

May 19, 2015

Chairman Neugebauer, Ranking Member Clay, and members of the Subcommittee, thank you for the opportunity to testify today on such a critically important topic. A large-scale cyber attack is likely the most significant and systemic threat facing our economy today so it is appropriate that so much time and energy is being focused on developing public-private partnerships and identifying solutions to mitigate that risk. For SIFMA[1] and its member firms, our mission is to improve the collective ability of our sector to defend against a diverse set of cyber threats and be proactive in protecting our firms' clients and trading partners in addition to their data and networks from theft, disruption or destruction. Our member firms have invested huge sums of capital into their cyber deterrence and protection programs over the years and have enhanced their efforts to match the growing threat. From criminals seeking financial gain, to nation states committing corporate espionage, to cyber terrorists seeking to dislocate markets and destroy confidence, cyber threat actors are becoming more sophisticated, making cybersecurity an area of risk that must be actively managed by firms similar to all other areas of risk. The destruction of financial data including books and records or the disruption of our capital markets caused by a successful cyber attack would have a ripple effect across the economy and across the globe. As such, the financial services industry welcomes the importance placed on this issue by the Administration and the Congress, as demonstrated by today's hearing and previous hearings in the Financial Services

[1] SIFMA is the voice of the U.S. securities industry, representing the broker-dealers, banks and asset managers whose 889,000 employees provide access to the capital markets, raising over $2.4 trillion for businesses and municipalities in the U.S., serving clients with over $16 trillion in assets and managing more than $62 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

Committee. As we focus on addressing the causes of the last financial crisis, it is equally if not more important that we focus on the future risks, and cyber is perhaps the greatest.

In order to insure adequate defenses and recovery protocols, it is critical that we establish a robust partnership between the industry and government as it is the most effective way to mitigate cyber threats: the industry will not be fully effective without the government's help, and vice versa.

For our part, SIFMA has recently undertaken a five-part effort to address cybersecurity threats and related risks to its membership of banks, broker-dealers and asset managers and the financial services industry at large. We have established a task force of 30 firms representing a broad cross section of the industry who are engaged in this work to ensure the unique interests and needs of institutions of all shapes and sizes are addressed. The ultimate goal of these five initiatives is to better identify the vulnerabilities for a cyber attack and prepare individual firms and the broader sector to defend themselves, thereby enhancing protections for the capital markets and the millions of Americans who use financial services every day.

Standards

Effective cybersecurity regulatory guidance is critical for both the financial services sector and the other critical infrastructure sectors we rely on. SIFMA commends the various regulatory agencies for conducting a review of their cybersecurity policies, regulations, and guidance and conducting surveys and sweeps of the firms that they cover with the goal of strengthening the defense and response of firms to cyber attacks and to better understand the investments that firms have already made to address this risk.

In addition to the reviews being conducted, we have suggested, via our published Principles for Effective Cybersecurity Regulatory Guidance,[2] that regulations be harmonized across agencies for greater effectiveness. Industry looks to the government to help identify uniform standards, promote accountability across the entire critical infrastructure, and provide access to essential information and SIFMA urges policymakers to consider how best to incorporate the principles into their respective regulatory initiatives.

SIFMA's principles build upon the highly valuable NIST Cybersecurity Framework—an initiative which we contributed much time and energy to and after its release, have sought out opportunities

[2] SIFMA Principles for Effective Cybersecurity Regulatory Guidance: http://www.sifma.org/issues/item.aspx?id=8589951691

to promote its use within the sector by mapping existing compliance requirements so firms can see where they could not only achieve risk management benefits but compliance benefits as well.

Likewise, government depends upon industry to implement regulation or guidance and collaborate on identifying risks and providing effective solutions to those highlighted areas. An illustrative example of this industry collaboration is how we are addressing the management of third party relationships and the cybersecurity risks that arise from them. A standardized set of controls and a process for implementing and evaluating those controls by third parties would foster greater transparency and confidence in a critical component of our overall ecosystem. Today, regulated utilities and service providers must answer various firms' non-standard requests for information on their cybersecurity practices and other critical areas. This information is important to all stakeholders, but is presently handled via a bespoke approach for vetting and auditing that is focused on data collection vs. active risk management. A consortium of 8 banks, 10 exchanges/utilities, and 4 audit firms is working towards streamlining the data collection process by building upon the AICPA SOC-2 criteria, the NIST Cybersecurity Framework and the specific requirements of the industry to create a control framework that is easier to execute, more comprehensive and increases the level of assurance that firms have in their thirds party providers.

Improving Resiliency in the Markets

Additionally, SIFMA assembled a working group to develop a diagnostic on the U.S. equity and Treasury markets. After mapping process flows within the markets, a workshop was held during which a set of 10 diverse cyber-risk scenarios were applied to the markets and a number of potential risks or vulnerabilities were identified. These results are being addressed via a number of public and private sector working groups. At a high level, the most important cybersecurity issues identified by the working group were the need for destructive malware defense and analysis capabilities, the development of cybersecurity standards for third party providers and the need for improved incident response coordination.

Incident Response

SIFMA's members refined the industry's crisis incident response plans to ensure that it is well tested and recognizes the appropriate role of our government partners. Building off the after-action reports and lessons learned from the cyber exercise "Quantum Dawn 2" and from our experience in

Superstorm Sandy, SIFMA developed and documented the protocols and process to create an industry consensus recommendation to respond to a systemic incident within the Equity and Fixed Income markets. To enable this process, SIFMA created two new market response committees covering these two markets, which will facilitate discussion and decision-making in the event of a crisis. In order to develop a comprehensive review and recommendation for an incident, these committees include SIFMA member firms, exchanges and utilities, securities regulators and Treasury as our sector specific agency. On October 24, 2014, SIFMA conducted a test of the process with extensive participation by both committees, resulting in an after-action report that will drive additional improvements. In support of the Financial Services Sector Coordinating Council (FSSCC), SIFMA launched a multi-faceted approach to engaging the government in order to facilitate a common understanding of how the capital markets will be supported in the event of an attack and what mechanisms and capabilities are available for defending the markets, and in turn investors, while re-establishing public confidence in the recovery.

This dialogue has evolved into a joint exercise program composed of quarterly table top exercises for both public and private sector firms and agencies to discuss the specific capabilities and response processes that would be executed in the event of a successful cyber attack against the financial industry. These exercises produce after action reports which are then used by the sector and Treasury to drive improvement and ensure we are prepared as an industry and nation to respond.

Insider Threat

As we have learned from recent events, the threat of breach and unauthorized disclosure can appear from both external and internal sources and both need to be actively addressed and monitored. Building upon a proactive approach to cybersecurity, SIFMA developed a set of best practices from a number of public and private sector sources to assist firms in the development of their own insider threat mitigation programs. This best practices guide provides context, considerations, and a method for implementation of an insider threat program that aligns with the NIST Cybersecurity Framework to facilitate integration into firms' cybersecurity programs and allow synergies to be leveraged as many risks overlap.

Information Sharing

SIFMA has worked to deepen our members' engagement with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and by experimenting with unique ways to drive membership. The FS-ISAC is the global financial industry's go-to resource for cyber and physical threat intelligence and a key operational component of the sector's defense. Its role is so central that on November 3, 2014, the Federal Financial Institutions Examination Council (FFIEC) recommended that financial institutions should join sector-wide information sharing organizations like the FS-ISAC. The FFIEC noted that "participating in information-sharing forums is an important element of an institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents." In line with this recommendation, SIFMA has funded a one year membership for 181 SIFMA members in the small firm category in order to achieve a near 100% membership overlap with FS-ISAC.

In addition to promoting information sharing, we have also sought ways to increase the level of cyber defense and readiness for small firms, by publishing a cybersecurity guidebook informed by best practices at larger institutions and government partners centered on the NIST Cybersecurity Framework. Looking into the future, SIFMA and its members are leaders in both the development and support of Soltra Edge, a software solution from DTCC and FS-ISAC that is designed to facilitate the collection of cyber threat intelligence from various sources, convert it into an industry standard language and provide timely information on which users can decide to take action to better protect their company. SIFMA sees Soltra as a significant step forward in sharing threat information at machine speeds within the sector and ultimately with other sectors, third parties and agencies of the US Government. This is another great example of the sector partnering and innovating at a rapid pace to address the cybersecurity risks we face and increase the costs for attackers.

Overall, there has been a marked improvement in information sharing between the financial sector and Law Enforcement, the Departments of the Treasury, and the Department of Homeland Security. Department of Justice anti-trust clarifications and improved turnaround time on security clearance approval requests have also better equipped information security officers with actionable information. A few aspects of the industry-wide cybersecurity effort, however, would particularly benefit from greater U.S. government involvement:

(i) More clarity on how roles of various USG authorities match up with specific aspects of cybersecurity

(ii) Higher quality and increased frequency of classified briefings to sector

(iii) Accelerated timing of security automation objectives

(iv) Accelerated timing of cybersecurity R&D initiatives

(v) Focus on attracting a wider cybersecurity talent pool / work force to address shortage

Furthermore, as I mentioned, there is a need for Congress to continue their productive engagement in this effort to improve our cybersecurity and the best place to focus is taking up and passing S. 754, the Cybersecurity Information Sharing Act (CISA) of 2014, which received large bipartisan support in the Senate Intelligence Committee this past March. While the House has done its part to move the ball forward, the threat our economy faces from cyber attacks is real and information sharing legislation will help the financial services industry to better protect our systems and data as well as the privacy of our customers. The financial services sector cannot wait for the next attack to get a bill to the President's desk and so SIFMA calls on the Senate to act on CISA and for the House and Senate to reach quick agreement through a conference. Congress must remain vigilant and proactive and provide the private sector with laws that will enable us to better protect ourselves and collaborate with our government partners.

Conclusion

Neither the industry nor the government can prevent or prepare for cyber threats on their own. SIFMA believes that a dynamic and collaborative partnership between the industry and government is the most effective path forward to accomplishing this goal. Among other areas for collaboration, government participation in industry exercises is critical to gain a better understanding of our collective capabilities in the event of a crisis. For Quantum Dawn 3 (QD3), we are currently planning for a major industry-wide exercise in Q3 2015. QD3 will build upon the breadth and success of QD2 and continue to focus on an attack on the US equity market that has a systemic impact. The exercise will include participants from the public and private sector and focus on how we collaborate during a crisis to maintain operations in the face of an attack.

As an industry, we have made cybersecurity a top priority. It is an issue my member companies worry about every day. SIFMA has brought together experts from across the public and private sectors to better understand the risks involved in a cyber attack and develop best practices to be better prepared to thwart an attack, but to be effective, we must work closely with the federal government to strengthen our partnership, protect our economy and the millions of Americans who place their confidence in the financial markets each and every day.

###