December 10, 2014

Statement of the Securities Industry and Financial Markets Association

Senate Committee on Banking, Housing, and Urban Development

Hearing Entitled "Cybersecurity: Enhancing Coordination to Protect the Financial Sector

In today's digital world, both the public and private sectors must improve their ability to defend against a diverse set of cyber threats and be proactive in protecting their partners and clients in addition to their data and networks from theft, disruption or destruction. From criminals seeking financial gain to nation states committing corporate espionage or 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 other areas of risk. The destruction of financial data 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. In that light, President Obama has stated that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity." SIFMA[1] and its member firms are leaders in developing and participating in the critical partnership between the government and the financial

[1] The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. 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.

services industry and appreciate the interest shown by this Committee and others in evaluating our collective efforts.

SIFMA has recently undertaken a five part effort to address cybersecurity threats and related risks to its membership and the financial services industry at large. The ultimate goal of this effort is to better identify the vulnerabilities for a cyber attack, improve the industry's cybersecurity protections and prepare individual firms and the broader sector to respond to a cyber attack, thereby enhancing protections for the capital markets and the millions of Americans who use financial services every day. More than 30 firms from across the industry are engaged in this work to ensure the unique interests and needs of institutions of all shapes and sizes are addressed.

Standards

Effective cybersecurity regulatory guidance is critical both for the financial services sector and the other critical infrastructure sectors we rely on. SIFMA commends the various 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 better understanding the investments that firms have already made to mitigate this risk. In addition to the reviews being conducted, we suggest via our recently published Principles for Effective Cybersecurity Regulatory Guidance[2] that regulations should be harmonized 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. Likewise, government depends upon industry to

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

implement regulation or guidance and collaborate on identifying risks and providing effective solutions. The guiding principles are designed to encourage regulation that facilitates a collaborative relationship and protects the financial industry for the overall security of investors and the nation's economy and SIFMA urges policymakers to consider how best to incorporate the principles into their respective regulatory initiatives.

Improving Resiliency in the Markets

We recently assembled a working group to develop a diagnostic on the U.S. equity and Treasury markets. The working group brought together a broad collection of market participants to identify risks and areas of concern around processes and technology. 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 were identified as a result. These results will be shared with the government and other industry stakeholders in order to jointly identify potential mitigating actions to address the identified risks and further improve equity and treasury market structure.

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 Superstorm Sandy, SIFMA developed and documented the protocols and process to efficiently create an industry consensus recommendation in response to a systemic incident within the Equity and Fixed Income markets. To enable this process, SIFMA created two new market response committees covering the markets above, which will facilitate the process in the event of a crisis.

On October 24, 2014, SIFMA conducted a test of the process with both committees. Participation from firms, exchanges, financial utilities and regulators was extensive and an after action from the exercise will likely be available at the end of December. This year, SIFMA also 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.

Insider Threat

Building upon a proactive approach to cybersecurity, SIFMA has developed a set of best practices 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. 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.

Information Sharing

SIFMA has worked to deepen our members' engagement with the Financial Services Information Sharing and Analysis Center (FS-ISAC) by promoting general membership and participation in its programs. 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 supportive in both the development and implementation 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.

Furthermore, there is a need for Congress to engage more productively in this effort to improve our cybersecurity and the best place to start is by the Senate taking up and passing S. 2588, the Cybersecurity Information Sharing Act (CISA) of 2014, which received large bipartisan support in the Senate Intelligence Committee this past July. The threat our economy faces from cyber attacks is real and Congressional action will significantly improve information sharing crucial to improving our cyber defenses. SIFMA believes the Committee has taken a balanced approach which will help the financial services industry to better protect our systems and data and the privacy of our customers. Congress should move swiftly. We cannot wait for the next attack to

legislate, but 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 September 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 a destructive data attack.

Another area where collaboration is critically important surrounds efforts to enhance regulatory harmonization beyond existing requirements to improve the protection of the financial sector. The benefits of this partnership approach led to the development of the NIST Cybersecurity Framework, which SIFMA is actively promoting within its membership and encourages regulators to use as a universal structure that can be leveraged as a starting point for creating a unified approach to cybersecurity.

As an industry, we have made cybersecurity a top priority. 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.

###