sifma
Invested in America

April 28, 2017

The Honorable Steven T. Mnuchin
Secretary of the Treasury
U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Re: Cybersecurity in the Financial Sector – Industry Concerns and Activities

Dear Secretary Mnuchin:

The Securities Industry and Financial Markets Association (SIFMA)[1] writes to you to provide our views on cybersecurity within the context of the President's Executive Order 13777, Enforcing the Regulatory Reform Agenda.[2] Specifically, our letter focuses on the need to ensure coordination among U.S and global regulatory and supervisory agencies, and the benefits to financial stability this will bring.[3]

Executive Summary

Cybersecurity has been called the greatest risk to the financial system.[4] Cyber risks have moved from discussions among information technology personnel to boardrooms[5] as business leaders must protect their clients, data, networks and operations from theft, disruption and destruction. From criminals seeking financial gain to nation states committing corporate espionage or seeking to dislocate markets, cyber threat actors are becoming more sophisticated in their attack methods, making cybersecurity an area of risk which must be actively and increasingly managed.

---

[1] SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over $2.5 trillion for businesses and municipalities in the U.S., serving clients with over $20 trillion in assets and managing more than $67 trillion in assets for individual and institution 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.

[2] Executive Order 13777, 82 Fed. Reg. 12285 (Feb. 24, 2017). See: https://www.federalregister.gov/documents/2017/03/01/2017-04107/enforcing-the-regulatory-reform-agenda.

[3] See: http://www.sifma.org/issues/item.aspx?id=8589965485, SIFMA Submits Comments to the Treasury on G20 Finance Ministers and Central Bank Governors (SIFMA Letter to Treasury).

[4] Lambert, Lisa and Baryln, Suzanne, *SEC Says Cyber Security Biggest Risk to Financial System* (May 18, 2016), REUTERS. See: http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4.

[5] Hiscox, *The Hiscox Cyber Readiness Report* (2017), at 15. See: http://www.hiscox.com/cyber-readiness-report/

The financial industry is committed to furthering the development of industry-wide cybersecurity initiatives that protect its clients and critical business infrastructure, improve data sharing between public and private entities and safeguard customer information. Effective and efficient cybersecurity policies will be achieved through coordinated efforts among industry stakeholders.

SIFMA has been and continues to lead coordinated efforts to support a safe, secure information infrastructure which provides security to customers and firms. SIFMA continues to work with industry and government leaders to identify and communicate cybersecurity best practices for firms of all sizes and capabilities, and uses its position to help educate the industry as to evolving threats and appropriate responses.[6]

Cyber defense, preparedness, and resiliency have been and remain foremost industry priorities. We believe the Federal Government should continue to prioritize cybersecurity, as the threat continues to grow. Actively addressing these issues will increase financial sector industry resiliency and inspire consumer confidence in industry capabilities. Specifically, we respectfully urge Treasury to support the following:

1. Use of the National Institute of Standards and Technology Cybersecurity Framework as a baseline for all future federal cybersecurity rules, regulations, or standards;
2. Harmonized cybersecurity regulation of the financial sector;
3. Use of the GFMA[7] penetration testing framework in all future federal rules, regulations or standards regarding penetration or similar cybersecurity testing or assessments;
4. Continued dialogue with industry working groups to improve data protection and cybersecurity at financial regulators and agencies; and
5. Sector-wide, joint public-private exercises.

SIFMA's comments focus on significant industry concerns regarding the: existence of multiple cyber preparedness frameworks; lack of regulatory harmonization; proliferation of risky penetration testing activities; the safety of private data submitted to financial regulators; and the industry's resiliency to potential cyber threat. The most overarching concern is the need for coordination among the multiple federal and state regulators and self-regulatory organizations (SROs). Below, we summarize the industry's current concerns, SIFMA's activities in remedying these concerns and propose how the Federal Government can further enhance cyber defense, preparedness and resiliency for the financial sector.

1. Use of the National Institute of Standards and Technology Cybersecurity Framework

The Federal Government has recognized that a need exists for a common, universal cybersecurity framework. In February 2013, President Obama issued Executive Order 13636, entitled "Improving

[6] SIFMA has developed cybersecurity resources for both the private and public sectors. See: http://www.sifma.org/issues/operations-and-technology/cybersecurity/resources/.

[7] The Global Financial Markets Association (GFMA) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London and Brussels, the Asia Securities & Financial markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.

Critical Infrastructure Cybersecurity."[8] That order directed NIST to develop – with the input of the private sector – a cybersecurity framework (the "NIST Framework" or the "Framework").[9] On February 14, 2014, NIST delivered this framework after conducting a series of workshops and obtaining stakeholder input.[10] The Framework is neutral as to technology and industry, and scalable as it "provides a common taxonomy and mechanism for organizations" to describe their current and target states for cybersecurity, "[i]dentify and prioritize opportunities for improvement," assess their progress, and "[c]ommunicate among internal and external stakeholders about cybersecurity risk."[11]

The Framework accomplishes these objectives by developing five core functions, each including multiple categories and subcategories that identify programmatic needs and technical or management activities to be considered.[12] Overall, it provides a means of creating and monitoring a risk-informed and adaptive information-security plan. As agencies coordinate, systematize, and organize their cybersecurity regulations and guidance as is generally directed by Executive Order 13563,[13] the NIST Framework offers the central organizing principles for cybersecurity protection.

The financial industry, including SIFMA's members, has supported the NIST Framework.[14] In its view, the Framework is a sensible and "flexible approach for all companies – large and small – to improve their cybersecurity procedures and their technical, administrative, and physical protections to the ever-changing threat" of cyber-attack.[15] Industry associations like SIFMA have thus helped their members and government agencies apply the NIST Framework.[16]

The NIST Framework, however, is merely suggestive, and the government has not required all agencies, including those supervising the financial sector, to organize their cybersecurity regulations in accordance with the Framework. In fact, numerous federal and state regulators have promoted the use of a competing framework developed by the Federal Financial Institution Examination Council (" FFIEC") – the Cybersecurity Assessment Tool ("CAT").[17] That tool, while potentially complementary and developed with the objective of building on the NIST Framework,[18] is far more prescriptive than the NIST Framework. The relevant agencies, states, and SROs, moreover, have not

---

[8] Exec. Order 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

[9] *Id.* § 7.

[10] Nat'l Inst. of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014) ("NIST Framework"), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[11] *Id.* at 4.

[12] *Id.* at 7–8.

[13] Exec. Order 13563, 76 Fed. Reg. 20568, 20569 (Apr. 13, 2011) (directing agencies to generally "consider the combined effects of regulations (together with those of other agencies) on particular sectors and industries" and "promote greater coordination across agencies, harmonization of regulatory requirements").

[14] SIFMA has worked with financial industry representatives and government agencies to develop and deploy the Framework's principles specifically for the financial sector. SIFMA has worked to map the NIST standards to cybersecurity requirements for financial firms.

[15] SIFMA, *Principles for Effective Cybersecurity Regulatory Guidance* 3 (Oct. 20, 2014).

[16] *Id.*

[17] FFIEC, *Cybersecurity Assessment Tool*, https://www.ffiec.gov/cyberassessmenttool.htm (last modified Feb. 13, 2016).

[18] *Id.* at App. B (mapping FFIEC Cybersecurity Assessment Tool to NIST Framework).

harmonized their regulations with either approach. Regionally, the New York Department of Financial Services released a final rule dictating prescriptive organizational and reporting requirements, unseen in any existing guidance or standards.[19] New York's foray into this area creates the threat of up to 50, disharmonized cybersecurity rules for financial institutions. The discord and confusion thus remains.

Coordinating financial-sector regulations into a unified approach, as noted above, would provide significant efficiency and help promote compliance. Government has expressed a need for collaboration and harmonization. For instance, then Deputy Treasury Secretary Sarah Bloom Raskin stated in 2016 that various regulators need to "figure out ways that we harmonize [cybersecurity standards]. We don't want to see emerge the development of multiple sets of standards, multiple guidances."[20] The financial industry also has advocated for financial regulators to coordinate with each other to avoid a counter-productive proliferation of overlapping standards.[21] The first action in such an endeavor is to catalog the key regulators and regulations to determine where overlap or conflict exists. This report seeks to accomplish that necessary first step.

The NIST Cybersecurity Framework,[22] developed as a result of Executive Order No. 13636 with the participation of over 3,000 cybersecurity professionals, is the hallmark of these efforts and represents the cybersecurity field's consensus on the most effective approach to improve cybersecurity.[23] Financial institutions have already designed cybersecurity programs to align with the NIST Cybersecurity Framework or other voluntary frameworks and comply with the FFIEC CAT and cybersecurity regulations promulgated under the Gramm-Leach-Bliley Act ("GLBA"), which also adopt risk-based approaches to cybersecurity.

SIFMA is scheduled to present at the May 2017 IOSCO[24] meeting, during which we will present on the state of cybersecurity and resiliency in the financial industry, the need for regulatory coordination, and support for risk-based frameworks including the NIST Cybersecurity Framework.

We ask the Treasury to support the use of the NIST Framework in all future regulator and agency rulemaking, standard-setting, guidance, and examination policies and procedures. Doing so may allow the industry to reach an ideal end-state, where U.S. cybersecurity standards impacting the financial sector are harmonized to the greatest extent possible. If each public-sector entity utilizes the NIST Framework as a baseline for future rules and regulations, with variation as necessary based

---

[19] New York State Department of Financial Services, 23 NYCRR 500. See: http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

[20] Lalita Clozel, *Regulators Must Improve Cybersecurity Coordination: Top Treasury Official*, American Banker (Mar. 17, 2016) (quoting Deputy Treasury Secretary Sarah Bloom Raskin), http://www.americanbanker.com/news/law-regulation/regulators-must-improve-cybersecurity-coordination-top-treasury-official-1079975-1.html.

[21] SIFMA, *Principles for Effective Cybersecurity*, *supra* note 15, at 7.

[22] Nat'l Inst. of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014) ("NIST Framework"), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[23] *See* Executive Order – Improving Critical Infrastructure Cybersecurity, E.O. 13636 (Feb. 12, 2013).

[24] IOSCO is the International Organization of Securities Commissioners, and brings together the "world's securities regulators and is recognized as the global standard setter for the securities sector." See: http://iosco2017mobay.com.jm/conference/iosco.php.

on the goals and remit of the regulator or agency, the industry will be able to more effectively utilize firm information security personnel, and limit the risks created by unharmonized standards and regulations.

2. Harmonized Cybersecurity Regulation of the Financial Sector

Financial institutions dedicate significant resources every day to measures designed to protect against cyber-crime, safeguard consumer data, and maintain the integrity and resiliency of their systems in the face of countless cyber threats. These defensive measures include developing information security plans, training employees, hiring experts to conduct risk assessments, and deploying defensive software and other technology solutions. Financial institutions also dedicate a significant amount of time and resources toward compliance with an expanding, and often overlapping, set of cybersecurity regulations**.**

Strengthening cybersecurity is a significant challenge shared by government and the private sector. That is especially true of the financial sector. Cybersecurity regulations and government guidance are not new. The Federal Government has long had a sector-specific approach to cybersecurity, meaning that different agencies and regulations govern different types of entities. And it has brought enforcement actions against companies with deficient protections that jeopardized consumer privacy and the soundness of critical infrastructure.

Each year, the financial sector expends significant resources to safeguard consumer data and protect against cyber-crime, a cost that can run as high as $500 million per year for the largest firms.[25] Entities large and small develop information-security plans and deploy all manner of defensive software. They train their front-line employees in basic best practices and hire experts to revise and further develop protective measures tailored to the specific needs of their firms.

Government likewise makes "[p]roactive and coordinated efforts … necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being."[26] In part, these efforts include building cyber defenses for the Federal Government's own systems and sharing information with financial institutions to allow them to best protect their networks.[27] They also include setting standards and regulations for the financial sector to ensure the protection of consumer information and the continued functioning of markets.

In the financial sector, the Federal Government's approach to cybersecurity is particularly fractured. The first cybersecurity requirements stemmed from the Bank Secrecy Act of 1970,[28] which "was designed to prevent money laundering, tax evasion, and terrorist financing."[29] This act required

---

[25] Steve Morgan, *Why J.P. Morgan Chase & Co. Is Spending a Half Billion Dollars on Cybersecurity*, FORBES (Jan. 30, 2016), http://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#211145fd2a7f.

[26] *Presidential Policy Directive/PPD-21*, *supra* note **Error! Bookmark not defined.**.

[27] Exec. Order 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

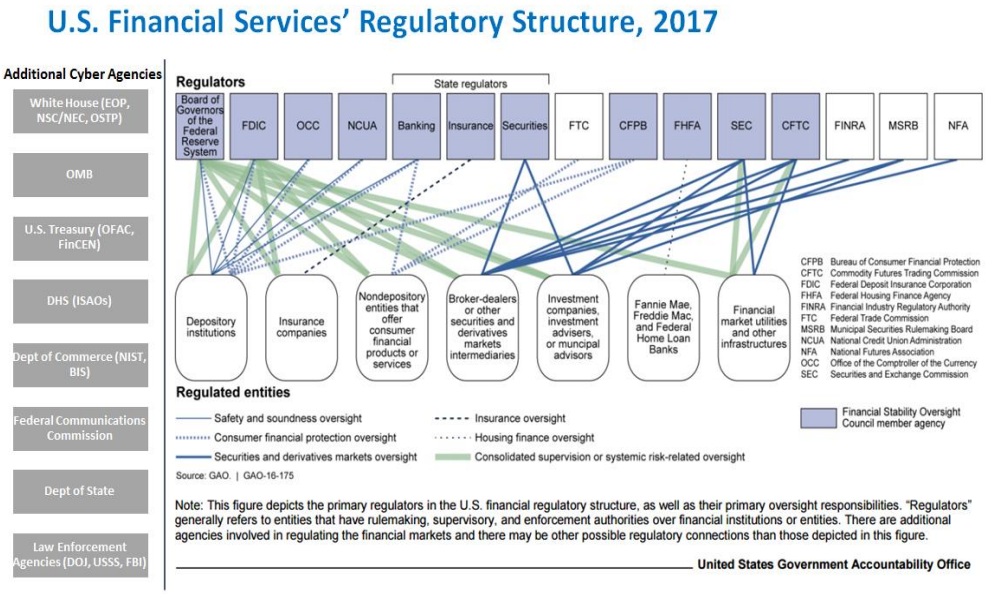
[28] Pub. L. No. 91–508, 84 Stat. 1114 (codified in various sections of Titles 12 and 15 of the U.S. Code).

[29] William A. Carter & Denise E. Zheng, *The Evolution of Cybersecurity Requirements for the U.S. Financial Industry* 2 (Jul. 2015).

financial institutions to "implement anti-money laundering IT management systems to prevent illicit transactions and account takeover, and to log and analyze customer information and account and transaction activity to detect suspicious behavior."[30]

Almost 30 years later, the Gramm-Leach-Bliley Act of 1999 ("GLBA") required financial institutions to adopt information security safeguards to protect the personal data of their clients.[31] The GLBA and the accompanying "Safeguards Rules"[32] promulgated by the Federal Trade Commission ("FTC"), National Credit Union Administration ("NCUA"), and the Securities and Exchange Commission ("SEC") require regulated entities to adopt written information-security programs designed to keep consumer data safe. Further, the GLBA authorized the Office of the Comptroller of the Currency ("OCC"), Board of Governors of the Federal Reserve, and the Federal Deposit Insurance Corporation ("FDIC") to promulgate Interagency Guidelines that similarly create standards for data protection.

The number of agencies and regulations governing the cybersecurity practices in the financial sector has only grown since GLBA's passage (see diagram below).



No fewer than 11 federal agencies impose some form of cybersecurity requirements on financial institutions today. Those regulations and guidelines are in addition to the individual states' requirements and those of self-regulatory organizations ("SROs"), such as the Financial Industry Regulatory Authority ("FINRA") and the National Futures Association ("NFA"). These regulations and guidelines are further supplemented by third-party standards developed and promulgated by the National Institute of Standards and Technology ("NIST") and the Federal Financial Institutions Examination Council ("FFIEC"), which guide agency examiners and financial institutions in setting cybersecurity standards and measuring the adequacy of cybersecurity programs. Each of these

[30] *Id.*

[31] Pub. L. No. 106–102, 113 Stat. 1338 (codified, in relevant part, at 15 U.S.C. §§ 6801–6809).

[32] 12 C.F.R. pt. 748 (National Credit Union Administration); 16 C.F.R. §§ 314.1–314.5 (Federal Trade Commission); 17 C.F.R. § 248.30 (Securities and Exchange Commission).

bodies mandates or strongly recommends that financial institutions maintain certain procedures, implement specific controls, or produce various audits or reports. Often, a single entity may be responsible to several agencies or organizations and associated set of overlapping requirements and standards.

The consequence of this multitude of regulations is potential confusion, redundancy, and incompatibility, and gives rise to possibilities for complicating compliance. For instance, a large commercial bank may be subject to the regulations or guidance of the Federal Reserve, the FDIC, and the SEC – each with potentially opposing directives. Its vendors, on the other hand, may be subject to the regulations of other agencies. The best practice in such a situation would be for the bank to insist that the vendor follow the regulations and guidance to which the bank is subject, but the vendor's unfamiliarity and potential lack of resources create the risk of unintentional noncompliance. Firms report that approximately 40 percent of corporate cybersecurity activities—which can include investments as high as $500 million per year for the largest firms—are compliance-oriented rather than security-oriented.[33] In other words, substantial resources are already being invested in complying with regulatory requirements rather than directly targeting security risks.

SIFMA, together with its global partner GFMA, the Global Financial Markets Association,[34] has long advocated for a harmonized, coordinated approach to cybersecurity. As discussed in our SIFMA Letter to Treasury, GFMA drafted the GFMA's International Cybersecurity, Data and Technology Principles[35] (the "GFMA Principles"), which were later adopted in part in the G-7 Principles and Actions on Cyber.[36] The principles offer the industry's approach to foundational elements for the formation of effective policy on cybersecurity, data, and technology. Further, SIFMA and other trade associations have convened a roundtable comprised of U.S. financial services regulators and SROs to discuss the impacts of regulatory discoordination in this area. SIFMA strongly encourages the Treasury to seek to coordinate and harmonize cyber rules and guidance among the federal financial regulators, and to the extent possible, with the state regulators and SRO's.

3. Penetration Testing

More recently, regulators, domestically and globally, are showing increased interest in **penetration testing** and other operational assessments such as network scanning and external monitoring of cybersecurity defenses. Such testing is a powerful tool to assess the success of financial institutions in safeguarding customers' data as well as infrastructure critical to the global economy. Regulatory bodies have a vested interest in the execution of the most realistic and rigorous assessments which utilize proven methodologies and yield unbiased data concerning the strengths and weaknesses of a firm's defenses. As a result, financial services firms, especially those which operate globally, are faced

---

[33] *See* PwC, Global State of Information Security Survey 2016 (Oct. 9, 2015), http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[34] See: http://www.gfma.org.

[35] See: http://www.gfma.org/correspondence/item.aspx?id=807. GFMA, EBF and ISDA Publish International Cybersecurity, Data and Technology Principles

[36] See: http://www.mofa.go.jp/files/000160279.pdf. G7 Principles and Actions on Cyber.

with an ever-increasing demand by regulators for technical insights into how they protect their customers' data, infrastructure and the results of conducted tests.

Regulatory compliance provides stability and confidence in financial markets that underpin the global economy; as such, the financial services industry has supported regulators' assessing and reviewing of cybersecurity programs. As the need for maintaining a robust cybersecurity defense system has grown, penetration tests and other operational assessments are becoming more focused on the systems themselves, rather than the controls around them, and have grown more complex, thus providing more granular data on firms' infrastructure and security posture. The increased use of penetration tests, as well as the depth of the tests, provides a benefit to regulators. However, this presents a risk to the firms and the firms' clients if the results become public or are inadvertently disclosed or stolen. Additionally, the increased use of disparate, possibly duplicative and prescriptive penetration testing methods and frameworks around the world demands increased resources within the industry to respond appropriately to each test; these required resources could be used more efficiently to protect firms and their clients.

A viable approach is required to address the regulators' need to evaluate security, while satisfying financial institutions' need for a scalable testing regime capable of improving their cyber defenses. To fill this need, SIFMA, together with GFMA and its regional affiliates, the Association for Financial Markets in Europe ("AFME") and the Asia Securities and Financial Markets Association ("ASIFMA") drafted a framework describing a safe, scalable method for conducting pen tests. We are also currently amid a global advocacy effort to socialize the framework with U.S. and global regulators and agencies. SIFMA, AFME, ASIFMA, and GFMA, together with global member firms have engaged in advocacy with U.S. regulators including Treasury, SEC, CFTC, OCC, as well as global bodies including the European Commission, Bank of England, Hong Kong Monetary Authority, Monetary Authority of Singapore, and the Dutch National Bank.

Cooperation between regulators and the industry will promote a safe, scalable and robust testing regime that is supportive of the evolving rules of multiple regulators, without introducing or exacerbating inherent operational and data risks. Regulators need to be provided with high confidence that the industry is meeting regulatory requirements through transparency in all phases. The industry needs a flexible framework established to perform realistic and rigorous penetration tests in a meaningful and efficient manner. The development of a global testing framework can address the respective needs of regulators and the financial industry, allowing for the continued confidence and growth of the world's financial markets and economy.

We propose the following key principles as the foundation for a commonly accepted framework:

- Provide regulators the ability to guide penetration testing programs at a high level, to meet supervisory objectives using common scenarios, agreed scheduling and scope of testing activities.
- Provide regulators high confidence that penetration testing is conducted by trained, certified personnel with sophisticated tools and techniques to accurately emulate adversaries.
- Provide regulators transparency into testing process governance for both regulator-driven and firm-driven testing, as well as assurance that firm governance provides that identified weaknesses are properly addressed.

- Ensure testing activities are conducted in a manner that minimizes operational risks and ensures data security to include regulators developing strict protocols for handling test findings due to the highly sensitive nature of this information.

The stability and safety of critical business processes, and the applications and infrastructure which support them, are of the utmost importance and are a national security concern. Disruption can jeopardize a firm's operations and its reputation, as well as adversely impact client data and confidence in the market. Penetration testing activities which seek to simulate real-world attacks against systems that support critical business functions can pose multiple risks, ranging from causing an actual breach, to the disruption of operations, to the consumption of excess firm resources. These risks, as outlined below, must be proactively managed via adherence to a robust set of risk management procedures that seek to achieve the objectives of both regulators and firms.

- *Multiple regulatory frameworks can result in unnecessary duplication of sensitive information, putting financial firms, their clients and other downstream third-parties at unknowable risk.*

Requiring firms to send sensitive data to multiple regulators dramatically increases the change of an unintended release of this data. Multiple regulator requests and disparate industry frameworks can lead to unnecessary duplication of findings and reports detailing firm vulnerabilities, whose details may be communicated and stored across multiples parties external to a firm. Permitting an outsized number of parties to hold this vital security information unnecessarily increases a firm's inherent risk, which is then passed on to firm clients, and third-parties. Testing data and reports provide a blueprint for exploiting a firm, and the loss of positive control of these results would be catastrophic. Beyond the impact to financial firms and firm clients, if data is lost or released concerning industry utilities or partners, this could adversely impact critical banking infrastructure upon which global markets depend.

- *Testing insights are reduced when regulators narrow options for test personnel and testing methods.*

The basic tenet of penetration testing is that, when performed correctly, the testers can accurately emulate adversaries and identify legitimate weaknesses in a firm's controls via a combination of new and innovate techniques that are developed at a pace far exceeding that of regulation or formal certification programs. Limiting the pool of available testers and the methods they employ will limit the ability of firms to rigorously test their security controls. The innovation and creativity of a sophisticated and highly trained penetration testing team is the primary benefit of using this testing method and limiting that by trying to use a single approach reduces this method's overall effectiveness.

- *Increasing regulatory requests requires testing teams to spend more time complying with requests and less time testing operational controls.*

Increasing levels of compliance activity could dilute testing capacity. Testing single systems or applications multiple times due to increasing levels of uncoordinated requirements, furthermore, results in duplication of efforts and risks. The need to comply with multiple requirements not only inherently increases the potential risk of data theft, loss or exposure, but adds operational overhead onto internal testing resources, and dilutes their capacity to conduct actual tests. This operational overhead, such as tracking requirements and integrating results into multiple reporting forms, has

the potential to overwhelm teams. The increased risk of a breach is magnified when teams must handle multiple files containing highly sensitive information, to the detriment of mounting a more robust cyber and operational defensive posture.

- *Multiple regulatory frameworks can result in inconsistent reporting.*

Much like the fact that multiple regulatory requests increase the operational overhead of compliance, multiple regulatory requirements for penetration testing will result in inconsistent reporting requirements.

- *Penetration testing of critical systems in production creates the significant potential to disrupt firm operations.*

The stability and safety of critical business processes, as well as the applications and infrastructure that support them, are of the utmost importance—as such a disruption can jeopardize firm operations and clients. Therefore, penetration tests seeking to simulate real-world attacks against these systems in production must be proactively managed via strict adherence to robust risk management procedures.

- *Creating multiple one-size-fits-all penetration testing frameworks disproportionately impacts midsize and smaller financial institutions.*

Penetration testing requirements can be onerous, even on large financial institutions. Establishing one-size-fits-all options rather than risk-based guidance ensures that midsize and smaller firms will have to devote an outsized percentage of resources for testing, rather than utilizing those same resources to improve and maintain robust, firm-appropriate controls. In the case of smaller financial institutions, it is generally beneficial for those firms to spend more on operations, including the detection and protection of firm infrastructure, rather than active testing. The negative downstream impact of forcing one-size-fits-all testing regimes upon smaller firms will inevitably impact firm clients.

We ask the Treasury to support the GFMA penetration testing framework, under which, financial institutions may conduct pen tests internally or utilize third-party vendors of their choice, then share the results of tests with their primary regulatory, with the full test results not leaving the financial institution. In exchange for permitting firms to conduct tests in this manner, firms will provide regulators the ability to guide tests to meet their supervisory objectives, provide regulators confidence that tests are conducted by certified professionals, provide regulators transparency into the test process and ensure that tests are conducted in a manner that minimizes operational risks. Adoption of the GFMA pen testing framework will ensure robust test programs, relative to the needs and scale of each firm, without undue risk of damaging firm operations.

4. Data Protection and Cybersecurity at Financial Regulators and Agencies

Maturing cybersecurity in the financial sector ecosystem is an important issue for regulated entities that provide significant amounts of sensitive information to federal agencies. SIFMA will seek to work with government partners to help improve the protection of industry data that they receive and hold.

In recent years, the Federal Government has demonstrated its commitment to cybersecurity by developing a more comprehensive legal framework for cybersecurity protections at federal agencies through the Federal Information Security Modernization Act ("FISMA"), and FISMA vests the Office of Management and Budget (OMB) with an important oversight role in determining benchmarks and working with agencies to measure their success in implementing laws and regulations pertaining to information security, and provides the Department of Homeland Security (DHS) with the authority to issue binding directives to agencies on actions needed to improve their cybersecurity. FISMA and OMB circulars have pointed to the NIST Framework for Improving Critical Infrastructure Cybersecurity as a metric to track the progress of agencies in improving their cybersecurity

We believe a collaborative approach to better data protection is critical to operating a strong financial sector. Over the coming weeks and months, we would like to work with our government partners to enhance and further open a dialogue regarding financial institution data protection. Working together, we can use our collective expertise to help understand risks and find ways to help each other secure the financial sector ecosystem.

5. Financial Industry Resilience and Exercises

Individual financial institutions have long recognized the need for internal cybersecurity protocols, and have developed intricate in-house playbooks to prepare for cyber-events. However, due to the U.S.' global economic importance, there arose a need for greater collaboration between the industry and the Federal Government.

The U.S. government, recognizing the need for increased public-private sector coordination and information-sharing released Presidential Policy Directive 41 ("PPD-41") in July 2016. PPD-41 calls for "sector-specific agencies to coordinate with critical infrastructure owners and operators to synchronize sector-specific cybersecurity incident response procedures."[37] Flowing from the PPD-41, U.S. Treasury circulated the draft Financial Services Sector Cybersecurity Enhanced Coordination Procedures ("CECP") describing the flow of information sharing between the public and private sector, invoking existing private-sector industry playbooks such as the SIFMA business continuity and market response processes and the FS-ISAC All Hazards Playbook.

To advance the financial sector's resiliency, the industry has organized large-scale exercises and tabletops to test and improve the sector's cybersecurity readiness.

- ***Hamilton Series***

SIFMA is an active participant in joint public-private exercises, including the "Hamilton Series." The Hamilton Series[38] is a set of joint public-private exercises which took place from 2014 through 2016.

---

[37] Presidential Policy Directive – Untied States Cyber Incident Coordination (July 26, 2016). See: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[38] Financial Services Sector Coordinating Council, *To Policy Makers in the Administration and US Congress* (January 18, 2017), at 3. See: https://www.fsscc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf.

The series involved collaboration between the financial sector and U.S. Government agencies to better prepare the financial industry for potential large-scale cybersecurity incidents. The exercises range from regional events among small and medium-sized companies, to cross border-tabletops, to sector-wide events hosted and led by the U.S. Treasury and Federal Reserve Bank of New York involving systemically-important financial institutions. The scenarios examine the impacts to different segments of the financial sector, which have included impacts to equity markets, depository institutions of all sizes, payments systems and liquidity, and financial exchanges.

SIFMA participated in the September 2016 Hamilton Exercise hosted by Treasury at the Federal Reserve Bank of New York. Discussion during the event focused on the processes in place when a destructive cyber-attack leads to a significant liquidity issue at a systemically important institution. We encourage Treasury, in its role as the critical infrastructure sector-specific agency for the financial industry to continue to coordinate and plan joint public-private sector exercises.

- ***Quantum Dawn***

In addition to participating in government-led activities, SIFMA acts as a leader for the financial sector in hosting and coordinating industry-wide exercises. SIFMA hosts a bi-yearly exercise titled Quantum Dawn, during which the private sector engages in a large-scale tabletop scenario involving large scale cyber-attacks.[39] The Quantum Dawn exercises are one major component of SIFMA's comprehensive work with our members on furthering the development of industry-wide cybersecurity initiatives.

Quantum Dawn I took place in 2011, and simulated simultaneous physical and cyber-attacks to test the response planning between financial firms and government agencies. Quantum Dawn II took place in 2013, and exercised a cyber-attack on the equity markets, combining multiple attack vectors from external and internal sources. Quantum Dawn III took place in 2015.[40] Quantum Dawn III was the largest industry exercise to-date with over 650 participants from 80 firms, , and involved combined cyber-attacks on the equity markets, post-trade infrastructure, and individual firms' data and systems.[41]

Quantum Dawn IV, scheduled for November 2017, is structured as a two-day event. Day will be a hands-on-keyboards exercise utilizing cyber-range technologies to allow participating firms' information security personnel to test their cyber risk mitigation capabilities in real time. Day two will focus on the industry and government-wide communications playbooks and will also allow firms to exercise all aspects of their internal response protocols. Exercise participants will include global and regional financial institutions, financial market utilities and infrastructure, regulators, agencies, SROs, and law enforcement agencies. In addition, Quantum Dawn IV observers will include global regulators, governments and standard-setting bodies.

SIFMA urges the Treasury to continue its robust engagement with the industry through coordination, table tops, and industry exercises.

---

[39] SIFMA, Business Continuity Planning. See: http://www.sifma.org/bcp/.

[40] SIFMA, *Cybersecurity Exercise: Quantum Dawn 3*. See: http://www.sifma.org/quantum-dawn-3/.

[41] *Id.*

Conclusion

Cyber-attacks are becoming increasingly sophisticated, more frequent, and their consequences dire. Robust cybersecurity defenses and incident response plans are now foundational elements for individual financial institutions, the financial sector, and the government agencies which support them.

Financial services firms spend millions of dollars on protection, investigation and remediation, and government agencies and regulators continue to publish and revise protocols, but more can be done. To effect positive changes for the benefit of financial services customers and firms, we restate the need for the public sector to add value to our efforts. We therefore restate the need for regulatory coordination and harmonization of future cybersecurity rules and regulations, and reiterate that we ask the Secretary and the Treasury to support:

1. Use of the National Institute of Standards and Technology Cybersecurity Framework as a baseline for all future federal cybersecurity rules, regulations, or standards;
2. Harmonized cybersecurity regulation of the financial sector;
3. Use of the GFMA[42] penetration testing framework in all future federal rules, regulations or standards regarding penetration or similar cybersecurity testing or assessments;
4. Continued dialogue with industry working groups to improve data protection and cybersecurity at financial regulators and agencies; and
5. Sector-wide, joint public-private exercises.

We hope you find this information helpful. We look forward to an opportunity to discuss our recommendations in more detail and look forward to working with you on these critical issues.

Sincerely,

Thomas Price
Managing Director
Operations, Technology & BCP

Cc: Craig Phillips, Counselor, U.S. Department of Treasury
Sarah Hammer, Director, Office of Financial Institutions Policy

[42] See: http://www.gfma.org.

Moses Kim, Deputy Director, Office of Financial Institutions Policy
James Sonne, Policy Advisor, Financial Stability Oversight Counsel

Gary Cohn, Director, National Economic Counsel
Andrew Olmem, National Economic Counsel

Randall Guynn, Partner, Davis Polk & Wardwell
Margaret Tahyar, Partner, Davis Polk & Wardwell
Luigi De Ghenghi, Partner, Davis Polk & Wardwell

Kenneth Bentsen, Jr. President, SIFMA