sifma
Invested in America

Principles for Effective Cybersecurity Regulatory Guidance

October 20, 2014

Effective cybersecurity guidance is critical for protecting the financial sector's data security and infrastructure. SIFMA commends agencies for conducting a review of their cybersecurity policies, regulations, and guidance with the goal of strengthening the financial sector's defense and response to cyber attacks, and harmonizing regulations and guidance for greater effectiveness. There is an opportunity to enhance agency guidance beyond existing requirements to enhance protection of the financial sector. 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 implement reform and collaborate on identifying risks and providing effective solutions. The guiding principles articulated below are designed to establish agency guidance that facilitate these relationships and protect the financial industry.

Today, SIFMA puts forward the following ten principles that should guide agency review and facilitate the dynamic partnership between financial regulators and industry that is essential for each to achieve their shared goals of protecting critical infrastructure and the assets and data of the public:

Principle 1: The U.S. Government Has a Significant Role and Responsibility in Protecting the Business Community

Principle 2: Recognize the Value of Public–Private Collaboration in the Development of Agency Guidance

Principle 3: Compliance with Cybersecurity Agency Guidance Must be Flexible, Scalable and Practical

Principle 4: Financial Services Cybersecurity Guidance Should be Harmonized Across Agencies

Principle 5: Agency Guidance Must Consider the Resources of the Firm

Principle 6: Effective Cybersecurity Guidance is Risk-Based and Threat-Informed

Principle 7: Financial Regulators Should Engage in Risk-Based, Value-Added Audits Instead of Checklist Reviews

Principle 8: Crisis Response is an Essential Component to an Effective Cybersecurity Program

Principle 9: Information Sharing is Foundational to Protection, Must Be Limited to Cybersecurity Purposes, and Must Respect Firms' Confidences

Principle 10: The Management of Cybersecurity at Critical Third Parties is Essential for Firms

Introduction

The threats to cybersecurity are well known. In 2013, the Director of National Intelligence, James Clapper, identified cybersecurity as the number one threat facing the United States for the first time.[1] FBI Director, James Comey, has since reinforced that "resources devoted to cyber-based threats will equal or even eclipse the resources to non-cyber based terrorist threats."[2]

The cybersecurity threat is present with an even greater urgency in the financial sector.[3] The recent series of attacks against businesses within the United States and the continuing threats to banks and financial institutions highlight the fact that financial companies face a persistent, evolving group of attackers with varying levels of sophistication and resources. In tune with the threat, financial institutions have been diligently working for years to increase and improve their own cybersecurity protections.

The type of threat actor financial institutions face varies widely. There are so-called "hacktivists" who attempt to bring down financial institutions' technology systems based on radical political and social beliefs, cybercriminals who steal personal financial details for sale on the black market, and state-actors who steal trade secrets and confidential information for their country's illicit economic gain. Adversaries are constantly changing their approach and as use of new technology mediums expand into mobile, cloud, and social media, the opportunities for a cyber attack grow as well.

Protecting Americans from the threat of a cyber attack, however, cannot be done by industry alone. The President, the National Institute of Standards and Technology ("NIST"), and agencies across the federal government have been leading the effort to encourage private sector critical infrastructure organizations to improve their cybersecurity practices. In February 2014, NIST

[1] "As more and more state and nonstate actors gain cyber expertise," stated Director Clapper, "its importance and reach as a global threat cannot be overstated." James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment to the House Permanent Select Committee on Intelligence (Apr. 11, 2013), available at http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/DNIWWT11April2013.pdf.

[2] James B. Comey, Jr., Director, Federal Bureau of Investigation, Senate Committee on Homeland Security & Governmental Affairs (Nov. 14, 2013).

[3] *See* Mandiant, *Not Your Average Cybercriminal: A Look at the Diverse Threat to the Financial Services Industry* (Sept. 23, 2013).

issued its final Cybersecurity Framework, a set of voluntary standards designed for critical infrastructure companies to use in developing a comprehensive cybersecurity program.[4]

SIFMA has taken a leading role in advancing the government's objective to use the NIST Cybersecurity Framework to reduce cyber security threats and encourage its adoption by members of the financial sector and their affiliates, vendors, and other essential third parties. The Framework provides a flexible approach for all companies—large and small—to improve their cybersecurity procedures and their technical, administrative, and physical protections to combat this ever-changing threat. SIFMA has worked with financial industry representatives and government agencies to develop and deploy the Framework's principles specifically for the financial sector. As NIST recently stated, such implementation of the Framework "will be essential as the marketplace becomes more focused on, and capable of, dealing with cyber-based risks."[5]

In this spirit of collaboration, we have articulated 10 principles to facilitate coordination and guide financial regulatory agencies in conducting their review. Because cyber threats are constantly evolving, the relationship between industry and agencies must be dynamic and collaborative.

Facilitating a Collaborative and Dynamic Regulatory Environment

We believe that a collaborative, dynamic approach to combat the cybersecurity threat is most effective. In a recent speech, FCC Chairman Wheeler articulated this vision for the communications sector by noting that agencies "cannot hope to keep up if we adopt a prescriptive regulatory approach. We must harness the dynamism and innovation of competitive markets to fulfill our policy and develop solutions."[6] Agencies and industry must work together to build this "new paradigm of proactive, accountable cyber-risk management."

[4] The Framework identifies five concurrent functions common across all critical infrastructure entities. All entities should develop the ability to: (1) identify cybersecurity risks and vulnerabilities; (2) protect critical infrastructure assets; (3) detect the occurrence of a cyber event; (4) respond to a detected event; and (5) recover from a cyber event. Framework Tiers characterize an entity's cybersecurity practices from partial (Tier 1) to adaptive (Tier 4) compliance. The Tiers are used to assess compliance with the Framework standards and legal and regulatory obligations, and to determine resource allocation. The Framework Profile aligns the Core's standards with the particular needs and practices of an implementation scenario. Companies can compare their current cybersecurity profile with their target profile to assess necessary steps to strengthen security. *See* NIST, Framework for Improving Critical Infrastructure (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[5] *See* NIST, Update on Cybersecurity Framework (Jul. 31, 2014), available at http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf.

[6] *See* Statement of FCC Chairman Tom Wheeler, as quoted by Allison Grande, FCC Head Prods Industry to Take Lead on Cybersecurity, Law360.com (June 12, 2014), available at http://www.law360.com/articles/547524/fcc-head-prods-industry-to-take-lead-on-cybersecurity.

This same approach applies with equal force in the financial regulatory environment. We embrace the Administration's efforts, as Secretary Jacob Lew stated, "to collaborate with the private sector to establish cyber security best practices and improve information sharing."[7] SIFMA has embraced this collaborative approach on multiple initiatives with the Department of Treasury.

Coordination is essential to enhance harmonization of regulatory guidance. The proliferation of different government and private sector security standards creates confusion and fosters an environment in which noncompliance is at risk. The focus of agency and Self Regulatory Organization (SRO) review, therefore, should be on harmonization of financial agency regulations and guidance across the federal government and with consideration of the international implications.

SIFMA suggests that an inter-agency harmonization working group may be useful to coordinate review of cybersecurity regulations and guidance and receive private sector input. The Office of Management and Budget (OMB) could facilitate this working group with White House approval to ensure that different agencies are talking to each other (including of course independent agencies and SROs), avoid unnecessary overlap, and build a coordinated response to improve cybersecurity. Another essential component to harmonization and consistency is ensuring that any domestic requirements are consistent with international legal obligations. An interagency working group could coordinate with international bodies, build ties with foreign regulatory authorities, and ensure that international requirements (in particular, those that derive from the EU Directive) are consistent with domestic obligations.

To help facilitate harmonization, we have attached the SIFMA cybersecurity framework that applies the NIST Cybersecurity Framework within the financial sector context. Flexible regulatory principles should grow out of such a framework to apply in a range of contexts to different firms of varied resources and vulnerabilities. Different agencies, of course, are assigned different responsibilities and jurisdictions. The principles articulated below encourage agencies to conduct their review by defining their respective roles and avoiding counter-productive overlap. One of the reasons that the NIST Framework's development was successful is that it is based upon collaborative input from the private sector and government. The same efforts should be devoted to the development of a successful regulatory regime.

The ten principles articulated here are designed to facilitate next steps to further build and solidify a collaborative approach to cybersecurity that can foster innovation and strengthen efforts to combat cyber threats to the financial infrastructure. As regulators work on new and updated regulatory guidance, these principles can serve as guideposts to focus attention, highlight points of common concern, and underscore issues that may result in unintentional harm to the financial sector.

[7] Remarks of Secretary Jacob J. Lew, Department of the Treasury, at the 2014 Delivering Alpha Conference (July 16, 2014), available at http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx.

The Principles

Principle 1: The U.S. Government Has a Significant Role and Responsibility in Protecting the Business Community

The U.S. government has capabilities that can significantly enhance all stages of a cybersecurity program. Though firms must rely on their own resources for cybersecurity, the federal government plays an essential role in assisting firms identify, protect, detect, respond to, and recover from cyber security threats and attacks. The government has access to the most up-to-date technology, malware information, and threat intelligence that can help safeguard the U.S. Moreover, all firms count on the enforcement of laws as a critical component to an effective cybersecurity program. The role of government is to prevent crime, and financial firms depend upon the vigorous enforcement of laws and actions against cyber criminals, whether state-actors or sophisticated cyber criminals.

The development of a collaborative environment requires recognition that firms are often the victims of cyberattacks and have an equal interest in combating cybercrime. Therefore, any resulting agency guidance should be crafted not to target the victims of such attacks, but to encourage the adoption of improved defenses and increased resilience. Firms targeted by attacks can suffer enormous, if not catastrophic, loss of intellectual property and information assets, and can lose the trust of its clients and customers. Industry should be viewed as a willing partner to encourage adoption of preventative and recovery measures.

Principle 2: Recognize the Value of Public–Private Collaboration in the Development of Agency Guidance

Each party brings knowledge and influence that is required to be successful, and each has a role in making protections effective. Firms can assist regulators in making agency guidance better and more effective as it is in everyone's best interests to protect the financial industry and the customers it serves.

The NIST Cybersecurity Framework is a useful model of public-private cooperation that should guide the development of agency guidance. NIST has done a tremendous job reaching out to stakeholders and strengthening collaboration with financial critical infrastructure. It is through such collaboration that voluntary standards for cybersecurity can be developed. NIST has raised awareness about the standards, encouraged its use, assisted the financial sector in refining its application to financial critical infrastructure components, and incorporated feedback from members of the financial sector.

In this vein, we suggest that an agency working group be established that can facilitate coordination across the agencies, including independent agencies and SROs, and receive industry feedback on suggested approaches to cybersecurity. SIFMA views the improvement of cybersecurity regulatory guidance and industry improvement efforts as an ongoing process.

Effective collaboration between the private and public sectors is critical today and in the future as the threat and the sector's capabilities continue to evolve.

Principle 3: Compliance with Cybersecurity Agency Guidance Must be Flexible, Scalable and Practical

Financial firms, both large and small, handle a range of different types of information with varying degrees of associated risks. Therefore, compliance with any guidance must be flexible and able to fit a range of different types of companies and business models. The blind application of prescriptive controls, while easier to track and understand, will not provide effective protection. An underlying risk calculus should be one of the primary drivers for implementation and firms should not be encouraged to implement ineffective and outdated controls.

Agencies should take the lead from the NIST Cybersecurity Framework, which is intended to be flexible and adaptive. Standards are developed and modified based on constant feedback and updating that takes into account real-world applications. As such, the Framework is "envisioned as a 'living' document, improved based on feedback from users' experiences, while new standards, guidelines, and technology would assist with implementation and future versions of the Framework."[8] The same should be true for the standards and practices recommended by agencies.

While there must be flexibility, a firm should not be deemed compliant by mere documentation of processes and controls. The application of cybersecurity guidance is an active, collaborative process and firms should apply resources to reduce risks. With such active participation, firms should be encouraged to develop different ways of protecting themselves via innovation.

Principle 4: Financial Services Cybersecurity Guidance Should be Harmonized Across Agencies

U.S. regulators and SROs, such as FINRA, should take a consistent and coordinated approach to cybersecurity that avoids redundancy and duplication of efforts. In offering a unified approach, agencies should use the NIST Cybersecurity Framework, which provides a universal structure that can be leveraged as a starting point. Indeed, it is designed to apply to all critical infrastructure sectors and entities within them.

SIFMA believes that any regulatory guidance developed out of this voluntary approach should provide flexible standards that can be applied across the financial industry to reduce cybersecurity threats. To encourage the adoption of such guidance, agencies should consider promoting a NIST Framework voluntary attestation protocol.

[8] *See* NIST, Update on Cybersecurity Framework (Jul. 31, 2014), available at http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf.

Regulators also should focus on guidance that is consistent with existing regulatory regimes and industry standards. Agency guidance should be harmonized with relevant ISO standards, Federal Financial Institutions Examination Council ("FFIEC") standards, NIST 800, Payment Card Industry ("PCI") standards, SANS Institute standards, Federal Trade Commission regulations and guidance, COBIT standards, international standards like the United Kingdom Cyber Essentials, and state standards like Massachusetts 201 CMR 17.

Financial regulators should coordinate to avoid a counter-productive proliferation of overlapping standards and overlapping regulators. A diffusion of regulatory principles undermines focus and diverts valuable resources for companies and agencies alike.

Providing a uniform approach allows firms that straddle different regulators to adopt the same fundamental guidance to developing cybersecurity policies and practices. This will save firms from executing multiple audits that cover the same content and shifting resources from security-focused activities. In addition, preparation would be consistent, which allows the reuse of documentation across multiple regulators. Regulators also benefit from sharing solutions to the same compliance problems. Consistency in regulatory guidance creates an environment in which all boats can rise.

SIFMA suggests that agencies establish a regulatory working group that could be facilitated by OMB to coordinate the review of guidance and regulations and provide an opportunity for industry to learn about efforts to increase cybersecurity and provide feedback. Such a working group also could coordinate with international regulatory authorities to ensure global consistency of cybersecurity regulatory requirements and advocate for an international approach that is consistent with domestic obligations. Independent regulatory agencies should agree to participate in an OMB working group on a voluntary basis.

Principle 5: Agency Guidance Must Consider the Resources of the Firm

Regulatory guidance for financial firms must take into account their size and resources. Sophisticated prevention measures are sometimes financially prohibitive for smaller firms and burdensome standards could drive these important players out of the market. The resources and technical sophistication of firms within the industry differ and the level of cybersecurity protection they can realistically afford varies. There must be flexibility in how firms protect their customers, with a focus on making the best use of the limited resources that may be available.

In large part, cybersecurity protections must be targeted to the threat. Firms should assess the systemic risk that they pose to the industry as a critical driver in the level of protection they should have in place. This should drive the firm's decision regarding the risks they are willing to accept and which risks should be mitigated.

Principle 6: Effective Cybersecurity Guidance is Risk-Based and Threat-Informed

Cybersecurity guidance simply cannot be "one size fits all." Rather, standards should depend upon multiple factors including: the type of information involved and its potential for harm, the size and resources of a firm, the unique risks associated with a company, the type of threats such firms face, the costs associated with implementation of security measures, the impact of compliance and whether customers will benefit, and the recent history of the types of harms that have transpired. Agencies should premise their guidance on a cost-benefit analysis that takes into account the benefits to firms and consumers versus the compliance costs and potential burdens suffered by consumers.

A firm's business model will dictate what aspect of information security (confidentiality, integrity or availability) is most critical to the delivery of services to their customers, protection of corporate assets and assurance of business continuity. As business models and the threat landscape change, agency guidance must be flexible to allow protections to evolve. Guidance must be targeted to the information type, potential for harm, and costs of protection.

The lack of a plan and program is no longer an option due to the interconnectedness of market participants and the flow of data. By the same token, firms should be discouraged from blindly applying ineffective controls without the use of a risk-based assessment to inform the firm's actions to protect their customers.

Principle 7: Financial Regulators Should Engage in Risk-Based, Value-Added Audits Instead of Checklist Reviews

Audit review is a fundamental component of the oversight and agencies have an important role to play. However, audits that firms spend a significant amount of time preparing for and executing should add value to help improve protections. Audits can add value by prioritizing items that focus on critical systems and sensitive data and are targeted to the particular business model of the firm. This will further encourage firms to embed a risk-based approach into their programs, instead of a checklist approach that provides minimal added benefit. The oversight provided by these audits is critical to ensure firms are adhering to their responsibility as a market participant and maintaining the trust that customers have in their financial institutions.

At the same time, regulators should increase the knowledge and skill of their examiners. This will result in an auditing process that is more consultative in approach as opposed to overly-strict compliance examinations that may or may not improve a firm's or the sector's collective security. Auditors from all regulators should be cross-trained to evaluate firms in a consistent manner, through a consistent process. Auditors also should seek to share and reuse information to assist firms in preparing for exams and audits.

In conducting their review and evaluating the value of agency guidance, agencies should engage in a cost-benefit analysis that could establish a *de facto* standard of care. Companies and agencies alike must evaluate the costs of instituting rigorous controls and cybersecurity threats along with the benefits of free information flows and increased security. For agency guidance to reflect the complexity of the environment, these types of tradeoffs must govern the application of standards.

Principle 8: Crisis Response is an Essential Component to an Effective Cybersecurity Program

No matter the strength of protections provided, it is possible that these protections will be compromised. Attention should focus on not just protections but also on the preparedness for response. Firms and regulators should be prepared to act immediately to stop access, isolate impacted information and systems, notify key partners, and conduct rapid damage control. In this process, firms must work with regulators and vice versa. Trust and confidence is essential to facilitate this dynamic and should be the objective of any agency guidance. Both firms and their clients are the victims when breaches or incidents occur. In short, there must be a greater focus on recovery efforts and resiliency, in addition to prevention.

Principle 9: Information Sharing is Foundational to Protection, Must Be Limited to Cybersecurity Purposes, and Must Respect Firms' Confidences

To protect information infrastructures, firms need access to real-time and actionable information. Similarly, the government needs access to information from critical infrastructure firms to provide insights into risks and associate risks across industries. We embrace efforts to increase information sharing, like the creation of the Financial Sector Cyber Intelligence Group within the U.S. Treasury and the continued evolution of DHS's National Cybersecurity and Communications Integration Center (NCCIC). Cybersecurity requires information sharing on a real-time, automated, and actionable basis.

Government and industry should utilize the promises that data analysis can offer in the context of cybersecurity. Threat trends and patterns can be more easily detected with a collaborative approach to information collection and sharing between government and the private sector and across critical infrastructure entities. This is why information sharing protections are so essential to facilitate this process. As these solutions are deployed, strong privacy and oversight protections must be built into the process.

Though the Department of Justice and Federal Trade Commission recently assuaged firms regarding antitrust concerns, firms need stronger legal protections that sharing cybersecurity information with other firms will not run afoul of antitrust concerns.[9] Regulators can assist in

[9] The joint statement from the Department of Justice and Federal Trade Commission reassures companies that sharing cybersecurity information will not run afoul of antitrust requirements. See Department of Justice &

making information sharing more effective by providing some level of safe harbor in disclosures. Agency guidance also should stress FS-ISAC membership as a key component to maintaining awareness and gaining an understanding of the threats that firms face.

Agencies should impose appropriate limitations on internal use and inter-agency sharing. One area of heightened awareness is the protection of privacy. Firms are, of course, under strict privacy regulations that derive from the Gramm Leach Bliley Act and Right to Financial Privacy Act, and consumers have come to expect that their personal information will be protected from disclosure. Financial firms cannot be viewed as agents of the government. Agencies, therefore, must establish procedures and regulations that limit the sharing of personal information provided by firms when such information is shared for cybersecurity purposes.[10] Personal information, for instance, should not be used by the government for independent and unrelated purposes to investigate individuals.

Similarly, so there is not a disincentive to share information, there must be restrictions on the government's use of information for other regulatory or enforcement purposes. The government should be prohibited from using such information for other regulatory or enforcement purposes. Shared information also should not be available for public release, civil discovery, or waiver of any applicable privilege.

These limitations on use will help to facilitate information sharing practices on a real-time, automated, and actionable basis. Firms need access to information to counteract threats, and government needs access to notify relevant players and coordinate responses.

Federal Trade Commission: Antitrust Policy Statement on Sharing Cybersecurity Information, available at http://www.justice.gov/atr/public/guidelines/305027.pdf. But more needs to be done. Sharing such information is critical to help mitigate and respond to cyberattacks.

[10] See Department of Justice: Sharing Cyberthreat Information Under 18 USC § 2702(a)(3), available at http://www.justice.gov/criminal/cybercrime/docs/guidance-for-ecpa-issue-5-9-2014.pdf:

> Improved information sharing is a critical component of bolstering public and private network owners' and operators' capacity to protect their networks against evolving and increasingly sophisticated cyber threats. As companies continue to adopt the newest technologies, these threats will only become more diverse and difficult to combat. Ensuring that information concerning cyber threats that U.S. companies detect on their domestic networks can be quickly shared will assist those companies in identifying new threats and implementing appropriate preventative cybersecurity measures. But sharing must occur without contravening federal law or the protections afforded individual privacy and civil liberties.
>
> We understand that the private sector would benefit from a better understanding of whether the electronic communications statutes that the Department of Justice (DOJ) routinely interprets and enforces prohibit them from voluntarily sharing useful cybersecurity information with the government. Companies have affirmatively expressed the desire to share information with the government, but have had questions about exactly what information may lawfully be shared. Overly expansive views of what information is prohibited from voluntary disclosure could unnecessarily prevent the sharing of important information that would be used to enhance cybersecurity, thereby thwarting opportunities to address a substantial challenge facing our modern society.

Principle 10: The Management of Cybersecurity at Critical Third Parties is Essential for Firms

Many of the systems and data stores within the critical infrastructure sectors reside not in the firms themselves, but in third-party service providers that are typically unregulated. Protections must be promoted at these non-regulated entities that the financial sector relies on. Similar to financial firms, third parties that pose a systemic risk to the industry should be identified, evaluated more closely, and encouraged to provide more information on the status of their cybersecurity programs. Regulators should increase their coverage of third parties and put pressure on these third parties to meet the regulatory expectations of the financial services firms that they serve.

Small- and medium-sized firms are particularly reliant upon third-party service providers. Many smaller firms outsource many components of their infrastructure, but lack the negotiating leverage to require third parties to implement robust cybersecurity protections. Agency oversight in conjunction with market forces should work together to ensure that such third parties implement these protections and do not leave the financial sector vulnerable.