April 29, 2013

Submitted electronically to: cyberincentives@ntia.doc.gov

Alfred Lee
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Washington, DC 20230

Incentives to Adopt Improved Cybersecurity Practices

Dear Mr. Lee:

The Financial Services Sector Coordinating Council (FSSCC)[1] appreciates the opportunity to provide comments in response to the Department of Commerce's Notice of Inquiry: Incentives to Adopt Improved Cybersecurity Practices,[2] and submits this response as a demonstration of the deep commitment the financial sector has to the public-private partnership envisioned by the Cybersecurity Framework, and the incentives that can aid in its adoption.

The financial services sector has been proactive in the development, adoption and implementation of best practices to protect their firms and the sector at large. The implementation of innovative technology and, effective mechanisms to allow for private to private sharing and partnerships with public entities to both inform and take effective action are just a few of the examples of how financial services has mitigated and managed the cyber risk that its firms are faced with on a day-to-day basis. Our number one existing incentive is the maintenance of trust. Financial services is built upon trust with our clients, trust between our firms and the trust to ensure the proper functioning of markets, the execution of transactions and the protection of information. It is the cornerstone of everything that we do.

To the extent that adoption of a Framework may be induced through incentives, FSSCC believes such incentives should be tailored to address specific gaps within the market or provide benefits to a sector (or a portion thereof). To be effective they must be compelling enough to affect corporate investment behavior and be adaptable across sectors and business functions, allowing for a menu of incentives and not mandating a one size fits all approach. In addition, the implementation of the Framework must provide benefits to firm's that adopt it by reducing their compliance costs and minimizing the risk of legal action based on its application. While the principles below provide a guideline for the incentives there are a number of challenges that the sector faced as it thought through the questions that were posed.

[1] A description of the FSSCC and membership listing is included as Appendix One.
[2] 78 FR 18954 (Mar. 28, 2013).

The main issue is the NIST defined Cybersecurity Framework does not exist. Hence, it is challenging for this sector, as well as others, to create a set of incentives to drive its adoption with the lack of clarity regarding what standard all critical infrastructure sectors may be held to or what new requirements, if any, will be added to those currently in place. NIST has stated it will consider the integration of standards "with existing frameworks," which FSSCC understands to mean that NIST will endeavor to complement and build upon the current cybersecurity standards adopted by the financial services industry. The financial sector is subject to a significant number of regulatory requirements, including federal and state laws and examination standards relating to cybersecurity, many of which emanate from the general financial safety and soundness standards and customer information security provisions contained within the Gramm-Leach-Bliley Act of 1999.[3] For example, depository financial institutions must comply with guidance produced by the Federal Financial Institution Examination Council (FFIEC). This guidance sets the standards for financial institution's information systems, outlining the minimum control requirements and directing a layered approach to managing information risks. To that end, in the absence of clarity FSSCC will be using existing standards and regulations to inform the discussion.

As referenced to above, incentives to drive the adoption of a Framework are important. It is not nearly as important as increasing the overall level of protection, readiness and resiliency across critical infrastructure. FSSCC believes the implementation of the Cybersecurity Framework can only be successful if the issues of information sharing, misaligned incentives, criminal penalties and access to government resources to defend against the threats of nation states are fully addressed.

The threat posed by nation states, in particular, is one that necessitates special attention. As the Framework is developed and implemented there needs to be an understanding that there are limits related to the expectations that can be placed on the private sector and that no level of incentives will allow a private company to create protections capable of defending itself from the unlimited resources of a nation state without the support of the federal government. In January 2012, Bloomberg and the Ponemon Institute released a study of six critical infrastructure sectors and reported on average that increasing private investment to prevent against catastrophic attacks would require a 900% increase in cyber security spending.[4] Of all the industries surveyed in the Bloomberg study, financial services would face the steepest increase in spending to reach an ideal state of protection. Financial companies' annual security costs would jump almost 13-fold on average to $292.4 million per company to fend off 95 percent of attacks, from the current $22.9 million, according to the study. Clearly this is unsustainable and uneconomical no matter what incentives are proposed. Therefore, it is our expectation that a successful incentive will make available the full capabilities of the federal government, including law enforcement, to defend and act as a deterrence against such nation state attacks.

FSSCC believes the timely sharing of threat information is critical to the government and the private sector in developing and deploying protective measures against malicious cyber activity. The Framework and the incentives should seek to enhance the ongoing efforts in this area by modifying outdated rules that currently constrain the private sector and government from sharing real-time information on threats and solutions. Existing information sharing and analysis mechanisms such as those provided by the Financial Services – Information Sharing and Analysis Center (FS-ISAC) play a vital role in incident response coordination, information sharing and other operational activities for the financial services sector. Improving and encouraging information sharing is central to protecting the financial services sector and the nation.

[3] Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338)

[4] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012

The final issue FSSCC addresses here is the fundamental misalignment between the incentives and disincentives between the attacker and the defender. There is an expectation that individuals, organizations or countries that engage in cyber attacks will not be caught and hence can continually attempt to breach the protections that firms put in their way until they are eventually successful in their attacks. In contrast, when an individual robs a bank, the expectation is that he or she will be caught and brought to justice, which is based less on the substantial precautions that banks undertake than upon the response of the local, state and federal government to enforce effective laws. Yet, the losses incurred by successful cyber attacks are usually impracticable to recover, and place financial institutions (and the country) at a disadvantage. Therefore, the incentives and disincentives must be brought into balance if any measure of efficacy is attainable in protecting critical infrastructure. FSSCC believes the prosecution of cyber criminals must be more effective at both the state and federal level and law enforcement must be provided the resources to more effectively deter and investigate these activities.

The proposed incentives below were drafted with the notion that cybersecurity is not a binary concept and cannot be applied in a one size fits all approach. Rather it is a sliding scale relative to what is appropriate, based on the specific risk perceived. This approach should likewise be applied to incentives. Because of limited resources the incentives should be focused on providing the greatest benefit, to the most critical of infrastructure components that address the most potent of risks to the nation as a whole. The financial services sector relies on the infrastructure of many of the other sectors to conduct our day-to-day activities and understands that by increasing their level of security and protections we also increase our own.

The following proposed list of 12 incentives is not provided in any order of priority and is organized based on the relevant categories.

1. **Grants**: Fund grants to the ISACs based on achievement of membership goals and the maturity of processes and procedures in place for information sharing. The goal is to drive uniformity and maturity across the sectors as the ISACs are incentivized to increase their collaboration on operational processes allowing for improved cross sector information sharing. The grant funds could be focused on the deployment of technology for analysis and automation.

2. **Grants**: Provide innovation grants to incent the development of new technology. A possible structure would be to establish a National Program Office (NPO) within NIST to manage grant applications and funded projects, similar to what was done for the National Strategy for Trusted Identities in Cyberspace program.

3. **Regulatory:** With the introduction of the NIST Cybersecurity Framework, FSSCC hopes to see a reduction in the number of regulations to which the sector must adhere. A possible solution would be a "Good Actor" benefit whereby firms that score well on a particular audit or review would then be granted relief for a period of time from other similar reviews done by other regulators. This incentive would drive significant cost and time savings as duplicative reviews are eliminated.

4. **Regulatory:** In order to drive the adoption of the NIST Cybersecurity Framework on a global basis FSSCC suggests that an active effort be made to harmonize the best practices, standards and regulations being considered with international ones that many of our firms are being measured against for operations outside of the United States. Along with the previous point, this incentive would reduce compliance costs, increase clarity in the face of conflicting regulations, and free up resources for improving security and addressing threats.

5. **Legislation**: Focus on passing laws that increase the penalties for cyber crimes, create a framework for increased international partnership among law enforcement organizations and focus on creating some

level of deterrent at the national level that will focus on nation states and sophisticated actors that have large scale capabilities to disrupt and destroy.

6. **Liability Protections**: Create a program similar to the Fraud Safe Harbor program but develop it specifically for the sharing of cybersecurity threat information. The program could, using established criteria, allow certified entities to engage in private to private information sharing with liability protections. This would enable some level of liability protection for certified firms but not require legislation for implementation.

7. **Liability Protections**: FOIA immunity for information shared with the Federal government. In addition, protections for the use and non-use of information that is shared from the Federal government to the private sector. Protection from negative regulatory action based on information obtained during information sharing. We view this as critically important to melding the public and private sectors interests on cybersecurity and to ensure that firms are incented to share information regarding attacks as soon as they occur.

8. **Liability Protections**: This incentive would encourage companies that are engaged in the implementation of bleeding edge technology and processes by mitigating the liability risk of adverse impacts caused by its implementation. This would increase collaboration between technology providers and their customers, increasing speed to market, ensuring new technology works as intended and cyber protection technologies employed by firms are the most advanced available.

9. **Liability Protections:** Any entity that complies with the Framework should be entitled to protection from liability for FTC or state attorney general actions arising out of events or breaches relating to these practices, as such compliance constitutes sufficiently responsible and reasonable "due care" behavior. Entities that engage in these security practices could be provided some litigation benefits relating to state common law actions arising from a breach in information security, which would serve as a deterrent to unexpected suits by creative plaintiffs' lawyers.

10. **Tax Incentive**: Develop tax incentives similar to SOP 98 which provides guidance in accounting for the expense or capitalization of costs for computer software developed or obtained for internal use. In this case, all costs associated with complying (e.g., time, hardware and software) with the NIST Framework could be considered tax deductible or amortized over a period of time thus providing a financial incentive for private sector entities to invest in Framework implementation.

11. **Tax Incentive**: Provide tax credits and/or deductions for critical infrastructure owners and operators and the firms that interface with their systems or networks who have also adopted the Framework. This would encourage the owners of these utilities to promote the Framework to firms participating on their networks (e.g. ACH), thereby increasing the overall security of the network and providing a tax benefit for all involved.

12. **Supply Chain & Procurement:** In order for the financial services sector to properly defend itself from persistent threats we need cooperation and collaboration from both the telecommunications and the information technology sectors. Known malicious content should be filtered from the Internet before being delivered to our networks. We expect less vulnerable products from our IT partners which are the foundation of our systems and networks. For ISP partners this means adding incentives to build service capabilities that mitigate threats before they enter the networks of their customers. For IT partners this means adding incentives to build secure software that is resilient to attack. If we are to stand a chance of defending the critical infrastructure within the financial sector we need incentives that will motivate these two partner sectors to increase the protections embedded within their products and services.

FSSCC believes the incentives listed above will help to drive the adoption of the Framework and improve the programs, processes, partnerships and technology relied upon to defend critical infrastructure. In conclusion, successful adoption of the Framework is but one step in effectively defending against cyber threats. FSSCC believes the federal government has a vital role to play in educating and incentivizing industry participants, retail and business customers, and counterparties regarding their roles in protecting against cyber threats. Increased education is an essential component of adopting any program and positively effecting individual and corporate behavior.

FSSCC thanks the National Telecommunications and Information Administration within the Department of Commerce for its efforts to develop incentives that will not only aid in the adoption of the Cybersecurity Framework but also improve our nation's cybersecurity posture. FSSCC welcomes the opportunity to meet with the NTIA, DHS or the United States Treasury to provide further insights into the financial services' views on incentives and protecting critical infrastructure.

Respectfully submitted,

Charles Blauner
Chair, FSSCC

Appendix One

Financial Services Sector Coordinating Council Membership

The Financial Services Sector Coordinating Council (FSSCC) fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council was created in June 2002 by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security activities in the financial services industry.

Associations	Operators	Utilities and Exchanges
American Bankers Association	Allstate	BATS Exchange
American Council Life Insurers	Bank of America	CLS Services
American Insurance Association	BNY Mellon	CME Group
ASIS International	Citi	Direct Edge
BAI	Equifax	DTCC
Bankers and Brokers	Fannie Mae	Intercontinental Exchange
BITS/Financial Services Roundtable	Fidelity Investments	International Securities Exchange
ChicagoFIRST	Freddie Mac	NASDAQ
Consumer Bankers Associations	Goldman Sachs	National Stock Exchange
Credit Union National Association	JPMorgan Chase	NYSE Euronext
Financial Information Forum	MasterCard	Omgeo
FS-ISAC	Morgan Stanley	Options Clearing Corporation
Futures Industry Association	Navy Federal	The Clearing House
Independent Community Bankers Association	Northern Trust	
Investment Company Institute	PayPal	
Managed Funds Association	Sallie Mae	
NACHA	State Farm	
National Association of Federal Credit Unions	State Street	
National Armored Car Association	Travelers	
National Futures Association	Visa	
SIFMA	Wells Fargo	