September 9, 2016

Via electronic submission to cybercommission@nist.gov

Ms. Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

RE: Recommendations to the Commission on Enhancing National Cybersecurity

Dear Ms. Grayson:

The Financial Services Sector Coordinating Council (FSSCC)[1] appreciates the opportunity to provide comments to the Commission on Enhancing National Cybersecurity (the "Commission") via the National Institute of Standards and Technology's (NIST) Federal Register request for *Information on Current and Future States of Cybersecurity in the Digital Economy*[2] (RFI).

To develop submission comments and recommendations, the FSSCC used a broad-based, cross-industry collaborative process that included participation from its member financial firms, utilities and exchanges, and trade associations, which, together, represent a cross-section of the financial services industry.[3] Essential to FSSCC's success is a commitment to public-private sector partnerships with executive branch and independent agencies, federal and state financial services regulators, and law enforcement agencies. Through these relationships, FSSCC has directed the sector's response to natural disasters, terrorist threats, and cybersecurity events.

[1] Established in 2002 by the financial sector, the FSSCC coordinates critical infrastructure and homeland security activities within the financial services industry. Its members consist of financial trade associations, financial utilities, and financial firms. The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the federal government, and coordinating crisis response - for the benefit of the financial services sector, consumers and the nation. More information about FSSCC can be found at www.fsscc.org.

[2] "Information on Current and Future States of Cybersecurity in the Digital Economy, Request for Information." *Federal Register*, vol. 81, 10 August 2016, pp. 52827-52829.

[3] FSSCC members are listed on its website at: https://www.fsscc.org/Member-Organizations. Aside from individual members of FSSCC, members from each of the financial trade associations that belong to FSSCC also participated. These trade association members can be found by visiting each association's website.

The cybersecurity topics referenced in the RFI are the same that shape FSSCC's collaborations with federal and state partners.

The Need for Public-Private Partnership to Address Cybersecurity Risks and Threats.

In 2016, the predominant cyber threat is human, a trait that has remained unchanged since the financial services sector provided its first set of recommendations to this Administration in 2009 via its Cybersecurity Policy Review.[4] Those recommendations highlighted a need for information sharing, and improved government support—several of which resulted in successful public-private partnerships. However, the sector now encounters a more sophisticated and dynamic threat that requires more mature collaborative processes, robust cross-sector support, and improved communication.

I. Cybersecurity Collaborative Accomplishments.

Since 2009, much has been addressed and accomplished through public-private collaboration, including many of the recommended items detailed in the 2009 letter.[5] The FSSCC would like to highlight a few of these cybersecurity successes.

A. The Development of the Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework").

When in February 2013, President Obama issued *Executive Order 13636, Improving Critical Infrastructure Cybersecurity,* directing that NIST develop a cross-sectoral voluntary cybersecurity framework[6], the financial services sector was wholly supportive. From the outset, the sector as a whole through the FSSCC has been significantly involved in the development of the *NIST Cybersecurity Framework,*[7] collaborating and participating in all six NIST cybersecurity workshops, including the most recent one in April 2016, and submitting responses to the various Federal Register requests for information.

Because of the open and transparent process that NIST utilized, private sector firms and government representatives provided undiluted feedback and engage in open dialogue concerning the *NIST Cybersecurity Framework's* strengths, weaknesses, and areas for improvement. This has not only resulted in a document that has been embraced from the

---

[4] Nelson, William B. "FS-ISAC Letter to Melissa Hathaway in Regards to the Interagency Cyber Security Review." 10 April 2009. Web. https://www.whitehouse.gov/files/documents/cyber/FSISAC%20-%204_10_09%20Public%20FSISAC%20Hathaway%20Letter.pdf *responding to* "President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review." Press Release. 9 February 2009. Web. <https://www.whitehouse.gov/the-press-office/president-obama-directs-national-security-and-homeland-security-advisors-conduct-im>.

[5] Nelson, William B. "FS-ISAC Letter."

[6] Obama, Barack. *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.* The White House, 12 February 2013. Web. <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

[7] Visit www.nist.gov/cyberframework for a copy of the framework and supporting materials.

operations floor to the boardroom, but also across enterprises, and across sectors. Additionally, because the *NIST Cybersecurity Framework* is applicable to all sectors and contains mapping to informative references, it operates as a *Rosetta Stone* translating sector specific risk management jargon and helps create a common understanding among the sectors of risk management terms and phrases. The common lexicon that it created, as well as the process used by NIST, should serve as a model for all future cybersecurity regulatory endeavors where public-private collaboration is essential.

B. Development of a Cyber Incident Severity Schema, Response Directive, and Deterrence Policy Tools.

The 2009 FSSCC letter stressed the need for the federal government to articulate its own cyber capabilities and engage in the diplomatic development of international cyber norms and deterrence strategies to mitigate against foreign-based threats and attacks. Since that time, the Administration, sometimes in consultation with the financial services sector and sometimes in coordination, has pursued indictments of nation-state affiliated attackers,[8] announced the creation of a cyber sanctions regime,[9] entered into cybersecurity memorandum of understanding with the Chinese government,[10] participated in cyber exercises, and most recently issued "Presidential Policy Directive – United States Cyber Incident Coordination" (PPD-41).[11] These necessary developments have provided a foundation upon which even more detailed and comprehensive government capabilities, norms, and deterrence tools can be built.

With respect to the recent PPD-41, the incident severity schema and incident coordination directives detailed therein are beneficial in that they articulate and clarify the roles and responsibilities of government actors, which, in turn, assists the financial services sector in preparing their own firms for cyber incidents and their own potential responses.

C. Cyber Threat Indicator Sharing and Analysis.

In a shared ecosystem with a persistent and dynamic threat, sharing and analysis of cyber threat information is essential for the defense of information technology systems and components. Accordingly, the financial services sector has, and continues to, advocate for

---

[8] United States v. Wang Dong, et al. United States District Court, Western District of Pennsylvania. *Indictment.* Criminal No. 14-118. Web. <https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf>; United States v. Ahmad Fathi, et al. United States District Court, Southern District of New York. *Indictment.* Criminal No. 16-48. Web. <https://www.justice.gov/usao-sdny/file/835061/download>.

[9] Obama, Barack. *Executive Order 13694 – Blocking the Property of Certain Person Engaging in Significant Malicious Cyber-Enabled Activities.* The White House, 1 April 2015. Web. <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.

[10] White House. "FACT SHEET: President Xi Jinping's State Visit to the United States." *Press Release.* 25 September 2015. Web. <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

[11] Obama, Barack. *Presidential Policy Directive 41 – United States Cyber Incident Coordination.* The White House, 26 July 2016. Web. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

mechanisms that increase such sharing and analysis. Collaborative accomplishments include the U.S. Department of Homeland Security-MITRE-private sector development of the STIX cyber threat language and TAXII transport protocol to enable automatic cyber threat indicator sharing,[12] the passage and signing into law of the Cybersecurity Information Act of 2015 to incentivize such sharing,[13] and the establishment of Treasury's Cyber Intelligence Group as per the sector's request.[14]

II. Recommendations to the Commission.

Despite these collaborative advances, there is much more that needs to be accomplished to mitigate against the increasingly advanced threats and other cyber risks. Through this submission, the FSSCC provides the following cybersecurity topic areas for consideration along with priority recommendations for action and improvement:

1) Federal government adoption of a forward-looking risk-based approach to emerging technology issue identification and attendant research and development;
2) Harmonization of cyber regulatory endeavors based on a common lexicon, such as the NIST Cybersecurity Framework;
3) Application of the risk-based approach in identifying and prioritizing essential sectors in the National Cyber Incident Response Plan;
4) Development of a national cybersecurity workforce; and
5) Enhancement of global and cross-sector coordination addressing cyber norms, deterrence, and response capabilities.

A. Federal Government Adoption of a Forward-Looking Risk-Based Approach to Emerging Technology Issue Identification and Attendant Research and Development.

Emerging technologies and services, such as Internet of Things (IOT) devices, web-enabled industrial control systems, mobile devices, cloud services, quantum computing,[15] and

---

[12] See https://stixproject.github.io/oasis-faq.pdf.

FSSCC would also like to note that STIX and TAXII enabled the development of Soltra. Soltra enhances the ability of financial services companies of all sizes to assimilate and analyze threat information—a capability that could be expanded to other sectors. This service decreases the time to decision and mitigation to hours or minutes. It does this by aggregating threat intelligence from a variety of sources, normalizing this data, and then prioritizing it at network speed, thereby turning it into instant actionable intelligence. For more information about Soltra, see: https://soltra.com/.

[13] Cybersecurity Information Sharing Act of 2015. Pub. L. 114-113. 18 December 2015. Web. <https://www.congress.gov/bill/114th-congress/house-bill/2029/text?overview=closed>.

[14] U.S. Department of the Treasury. "In Call to Action, Treasury Secretary Lew Urges U.S. Financial Sector to Redouble Efforts Against Cyber Threats." *Press Release.* 16 July 2014. Web. <https://www.treasury.gov/press-center/press-releases/Pages/jl2571.aspx>.

[15] An example of vulnerability arising from technological advance is the concern surrounding post-quantum cryptography. The construction of a production-scale (ca. 1000 qubit) general purpose quantum computer has the potential to irreversibly compromise every public-key cryptosystem in commercial use. Due to significant recent

wearable technology, etc., should be more fully examined and recognized for not only their societal benefits, but the unique cyber risks that they may pose. With the growth in connected devices and remote services, the potential for an increased attack surface that could be leveraged by bot-nets and those that control them is real. In a time of limited funding,[16] the federal government should appropriately fund research and development initiatives that not only identify these emerging technology issues, but also the risks posed and potential solution sets to mitigate these risks.[17] This may require a governmental cultural shift in thinking, funding, and coordination among government agencies that more closely resembles private sector partnerings (e.g., FS-ISAC, EWS) and risk-based prioritizations. Moving to such a forward-looking, risk driven posture would require an iterative approach that evaluates existing capabilities and controls in comparison to future capabilities, threats, and adversaries, including emerging technology and horizon vulnerabilities. The FSSCC would welcome an opportunity to discuss this recommendation further, including specific risk mitigation activities for specific technologies.

B. Harmonization of Cyber Regulatory Endeavors Based on a Common Lexicon, Such as the NIST Cybersecurity Framework.

In the two and one half years since the creation of the NIST Cybersecurity Framework, financial services agencies and self-regulatory organizations at the federal and state level have issued or proposed over thirty different frameworks, questionnaires, rules, and requirements related to cybersecurity. Although some of these cyber initiatives have incorporated the NIST Cybersecurity Framework's structure and terminology, others have not done so, opting for differing framework approaches and language.[18] With these disparate approaches in structure and language, the ability of firms to contextualize key issues and appropriately evaluate the effectiveness of internal and external cybersecurity efforts have been negatively impacted. The lack of harmonization and alignment are causing firms to expend substantial resources reconciling unique, and often competing, examination questionnaires, frameworks, and tools. Indeed, as an example, one multinational financial services firm reported that approximately

---

progress in both the science and engineering underpinnings of quantum computing, a production-scale quantum machine may exist within the next 10 years.

[16] While the FSSCC recognized that we are in a time of limited funding, it contends that current funding levels for federal cybersecurity research and development and cybersecurity initiatives, generally, are quite insufficient and do not match the risks posed. For example, the Administration proposed cybersecurity budget for 2017 was $19 billion (see: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan). By comparison, the development costs for F-35 Joint Strike Fighter are nearly $400 billion for only 2,457 planes. To further maintain these fighters, the Pentagon is expected to invest $1 trillion (see: http://www.cnn.com/2016/04/26/politics/f-35-delay-air-force/). If cybersecurity risk is among the nation's most serious risks (see: http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/), then funding should be commensurate to address that risk.

[17] To address issues related to industrial control systems and associated IoT devices, the FSSCC recommends increased funding for the ICS-CERT to carry out these activities. With respect to software security, the federal government should explore "language-theoretic security" or "langsec" approaches. Growing academic research suggests that by using such approaches it may not only reduce the likelihood of "weird machines" inside software code, which attackers can then exploit to execute their own code.

[18] For a list of examples, see: http://fsscc.morwebcms.com/files/galleries/NISTcommentletterSigned-0001.pdf.

40% of its cybersecurity efforts are expended on reconciliation and compliance, not on actual cybersecurity activity. More specifically, the resources spent to parse, identify, draft and compile equivalent data from similar systems multiple times for different regulators distracts limited personnel from actual security. This overlap has directed limited resources to creating single-use, compliance data sets, rather than expanding active security and mitigation.

To improve the national cybersecurity posture, the use, promotion, and establishment of a common cybersecurity lexicon and framework is crucial. A common approach assists internal communications among corporate cybersecurity professionals from the control room to the boardroom, and also supports external communications with other firms, sectors, and regulatory agencies. This commonality allows firms to respond efficiently to regulatory requests, to re-use and update answers when appropriate, and importantly, to focus resources on improving security capabilities. The Commission should recommend that all federal and state agencies pursue and adhere to a common lexicon, such as the NIST Cybersecurity Framework, when pursuing current and future cybersecurity regulatory endeavors.

C. Application of the Risk-Based Approach in Identifying and Prioritizing Essential Sectors in the National Cyber Incident Response Plan.

While the *National Infrastructure Protection Plan*[19] enumerates sixteen different critical infrastructure sectors, the federal government should further refine this list to a set of essential "lifeline" sectors for the purposes of the National Cyber Incident Response Plan. The creation of such a subset is an acknowledgement that the listed sectors are strategically essential based on their relative importance to the national economy, communications, or public health and safety. This subset, which would include the energy, telecommunications, and financial services sectors, should make them eligible to receive enhanced government assistance and support, such as supplementary intelligence, prioritization in emergencies, and additional liability protections to protect vulnerable downstream high risk, high criticality civilian infrastructure.

D. Development of a National Cybersecurity Workforce.

The well-known and well-researched shortfall in cybersecurity professionals is a national security and sector concern.[20] To encourage a robust cybersecurity workforce, the sector suggests that the development of skilled cybersecurity professionals become a national effort leveraging existing programs that demonstrate promise, but that could be improved over the short term and long term.

---

[19] The Department of Homeland Security's *National Infrastructure Protection Plan* (NIPP 2013) outlines how government and critical infrastructure private sector participants work together to manage risks and achieve security and resilience outcomes < https://www.dhs.gov/national-infrastructure-protection-plan >.

[20] According to the 2015 (ISC)2 "Global Information Security Workforce Study," the estimated 2016 shortfall of cybersecurity professionals in the Americas is 271,000 people. These estimates increase each year: for 2017, the shortfall is to 389,000; for 2018, 516,000. See: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf . Anecdotally, these numbers parallel reports of FSSCC members of hiring difficulties for cybersecurity professionals.

1. ***Improve Awareness of National Initiative for Cybersecurity Education's (NICE's) National Cybersecurity Workforce Framework.***

In 2010, the Administration established NICE and tasked NIST with overseeing the NICE program and coordinating stakeholder engagement. In the years since its inception, NICE developed and published the *National Cybersecurity Workforce Framework* (Workforce Framework).[21] The Workforce Framework is a progressive step in bridging the translation gap between cyber experts and employers by categorizing and standardizing job functions and descriptions for cybersecurity. Potentially, the Workforce Framework could improve job candidate selection and reduce vacancy time for job openings. However, the framework's usefulness is impeded by a lack of awareness among employers, information technology, and security recruiters. To improve awareness of this well-crafted tool and to reach one of its primary intended audiences, FSSCC suggests that NICE conduct targeted public outreach of the Workforce Framework to the recruiter community by participating in recruiter education events, conferences, and trade association meetings.[22]

2. ***Enhance Training and Education to Better Reflect Private Sector Workplace Requirements.***

While the National Security Agency (NSA) National Centers of Academic Excellence (CAE) were established to further the intelligence community's mission, they have evolved through partnership with the Department of Homeland Security (DHS), a civilian agency, to further the cyber defenses of the private and public sector.[23]

Under current accreditation requirements, participating colleges and universities must offer courses that align to specific cybersecurity-related knowledge units.[24] These requirements are technical in nature and do not adequately emphasize the other "soft skills" that are needed in the current and future workplace.[25] Such "soft skill" training and course requirements in problem solving, teamwork, conflict resolution, and the ability to translate technical concepts into business terms should be made mandatory for CAE certification.

---

[21] For more information about the NICE *National Cybersecurity Workforce Framework*, visit <www.csrc.nist.gov/nice/framework >.

[22] Additionally, FSSCC suggests that NICE update its website to make it more contemporary and easier to find the Workforce Framework, other supporting materials, and pertinent contact information.

[23] This broader focus is reflected in the 80% of graduates entering private sector service.

[24] National NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense. "CAE IA/Cyber Defense Updated Academic Requirements." Web. <https://www.iad.gov/NIETP/documents/Requirements/CAE_IA-CD_KU.pdf>.

[25] Financial services firms indicate that these skills, which are essential to the modern workplace, are often lacking in job candidates and new hires, making a difficult hiring process even more difficult. This problem is not unique to the financial services industry, however. A recent 2015 manufacturing sector survey indicated that less than half of respondents felt that their employees had "sufficient basic employability skills (attendance, timeliness, etc.) and the ability to work well in a team environment." 69% of respondents also reported that their employees lacked problem solving skills (see: http://www.themanufacturinginstitute.org/~/media/827DBC76533942679A15EF7067A704CD.ashx).

3. ***Refocus K-12 Efforts***.

FSSCC suggests that the federal government collaborate with the private sector and the state and local governments to develop age and audience appropriate materials targeted to K-12 students (and the guidance counselors that serve them) that articulate not only potential pathways to a cybersecurity (or STEM) related career, but the various "on" and "off ramps" available along the way. Since NIST's NICE lists similar objectives in its Strategic Plan,[26] the FSSCC suggests that with appropriate funding, NIST may be best positioned to convene the appropriate stakeholders and develop career pathway materials.[27]

E. Enhancement of Global and Cross-Sector Coordination Addressing Cyber Norms, Deterrence, and Response Capabilities.

In response to a global dynamic threat, the FSSCC recommends greater international (including international standards development organizations[28]), cross-sector collaboration, and information sharing with foreign governments.

1. ***Global Collaboration Addressing Norms and Deterrence***.

This collaboration would extend to the development of cyber norms, rules of the road, and agreements to pursue bad actors and botnet takedowns, including extradition treaties, within a streamlined international response. PPD-41[29] is a useful initial attempt to integrate a broader physical response to a cyber incident through a national response and preparedness system. A comprehensive and forward-looking national response should be coupled with a global collaborative component, and funding of cyber defense capabilities commensurate with the risk posed to national and international security.[30]

2. ***Interdependent Cross-Sector Coordination and Enhanced Information Sharing***.

The financial services sector has a longtime focus on prioritizing cross-sector information sharing to better reflect the reality of an interdependent matrix of critical infrastructures, across sectors and organizations. To develop a vehicle for responding to a significant disruption among sectors, the financial services sector, communications sector, and electricity subsector began

---

[26] See Objectives 2.3 and 2.5 in NICE's Strategic Plan, which can be found at: http://csrc.nist.gov/nice/about/strategicplan.html.

[27] FSSCC also suggest that future Administration and Congressional policymakers should review the data collected for the 2009 Department of Education longitudinal study of high schoolers and their course and career selection vis-a-vis STEM and craft future policy recommendations accordingly. See: https://nces.ed.gov/surveys/hsls09.

[28] Collaboration with international standards development organizations also has the benefit of being consistent with NIST's "Cybersecurity Framework Feedback: What We Heard and Next Steps," released in June 2016. See: https://www.nist.gov/sites/default/files/workshop-summary-2016.pdf.

[29] See footnote 11.

[30] The Administration's cyber budget of $19B is not equal to the task of preventing and combating nation state attacks. See footnote 16 for greater detail.

efforts in 2016 to collaborate on the development of enhanced procedures and a senior level coordinating council-level committee.

Further recommendations to enhance cross-sector coordination are:

a. A shared operating picture of critical infrastructure/key resources (CI/KR) areas. The financial services sector, and has limited visibility into the cybersecurity status of those sectors on which it is dependent, such as telecommunications, energy, and information technology.

b. Real-time information sharing and the development of cybersecurity response, notification, and collaborative take-down initiatives.

c. Cross-sector information sharing extended to third party and Nth party assessments. Third party management is costly and inefficient due to inability to share information, and entity-by-entity scoping.

d. Sharing vulnerability notifications and response management for companies, by sector and across sectors.[31]

III. Conclusion.

As we look over a 10-year horizon, the FSSCC and financial services sector remain keenly supportive of continuing our collaborative efforts on public-private initiatives to improve the nation's, and our sector's, cybersecurity stance. We believe that this collaboration is a critical national imperative, one that can only be successful with our combined and full focus. Through our collective work, we remain encouraged by the progress and advances of these joint efforts.

In light of the rapid pace of change in the cybersecurity arena we also see an accelerating need for faster development of key programs, more nimble response to policy, regulatory and critical infrastructure protection. And as referenced above, these will need the full commitment to resource and apply our most capable expertise. This need now encompasses multiple sectors and a more international landscape to be effective. With reference to examples of work already completed, our ability to identify meaningful programs and to set our focus and major investments to support them across government and private sector environments will be the standard and benchmark of our success.

If there are any questions or concerns about any of the recommendations made herein, please feel free to contact me or Brian Tishuk, Executive Director of the FSSCC.

Sincerely,

Rich Baich
Chair, Financial Services Sector Coordinating Council
Tel 704-715-8018
Fax 704-383-8129
rich.baich@wellsfargo.com

[31] For example, sharing cross sector cyber scenarios for lessons learned and proactive enhancements to response plans.