Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr.
Suite 230
Reston, VA 20191

January 18, 2017

To: Policy Makers in the Administration and US Congress
Subject: Financial Services Sector Cybersecurity Recommendations

The Financial Services Sector Coordinating Council (FSSCC) urges the Administration and US Congress to adopt these recommendations to further improve the cybersecurity posture of our nation. Attached is a brief summary of major accomplishments and initiatives to build on. With an estimated 85% of the nation's critical infrastructure in private sector hands and ever-advancing cyber threats, it is critically important that the public and private sectors continue to collaborate to address these threats.

Improvement Areas

1. **Invest Further in Financial Services-Supporting Infrastructure and Risk-Based Cyber R&D**
    - Ensure strong investment in the cybersecurity and resiliency of key Federal organizations, processes and systems essential to the functioning to the financial services system.
    - Ensure clear assignment of responsibilities and significantly stronger resourcing for efforts to detect, analyze and mitigate cyber threats to the financial system. This includes a dedicated effort within the Intelligence Community and an operational-level contingency planning, indications/warnings, and exercises program.
    - Fund cybersecurity defense and R&D initiatives commensurate with the risk that cybersecurity threats pose to the nation's security, including funding to identify risks and mitigation techniques for emerging Internet-of-Things (IoT) and quantum computing technologies.
2. **Pursue a Holistic and Streamlined Approach to Cybersecurity Regulation**
    - Encourage federal and state governments to adopt risk-based, streamlined and harmonized approaches for cybersecurity requirements that leverage the NIST Cybersecurity Framework and reduce the cost of translating and mapping to different requirements.
        - In 2013-14, government and private sector experts successfully collaborated on the development of the NIST Cybersecurity Framework. Since that time, financial services regulators have issued 30+ requirements, proposals, frameworks, and mandatory guidance. According to a recent survey, security professionals in the financial services sector now spend over 40% of their time translating and mapping these different requirements to the NIST Framework and other frameworks that they have in place to address cybersecurity – that's 40% of time not devoted to actual security.
    - Support a consistent and strong data protection and breach notification law across state and national platforms.
3. **Establish Global Cyber Norms and Cyber Deterrence and Response Capabilities**
    - Articulate how the US Government will respond to certain types of attacks and how these actions might impact the financial services sector and other critical infrastructure sectors. Pursue increased efforts for the extradition of cyber criminals. Attacks on the financial services industry and critical infrastructure should be considered a violation of an explicit global norm; violations of this norm should be pursued vigorously.
    - Enable and expand cross-sector, real-time and actionable cyber threat information sharing and situational awareness. Raise awareness among US Government agencies of existing policies and procedures (e.g., Critical Infrastructure Threat Information Sharing Framework) to ensure that the government is better coordinated.
4. **Prioritize Essential "Lifeline" Sectors in Planning and Event Response**

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr.
Suite 230
Reston, VA 20191

- Focus federal resources to assist those sectors whose operation is fundamental to the national defense and economy, such as financial services, electric power and telecommunications, to mitigate against cyber threats and to help in recovery. Continued private-public collaboration is required to develop the list of cyber defense capabilities that can be used to respond to a significant cyber incident affecting the nation's critical infrastructure.
- Ensure that the relevant members of the lifeline sectors receive the appropriate security clearances. Also, seek improvements in sharing classified information, passing clearances, and collaborating with the private sector in a classified environment.

5. **Develop a Technology Capable Workforce**
   - Partner with the private sector and academia to develop education and training programs to meet the business needs of today and tomorrow in addressing the significant shortage of cyber security professionals and the education system in producing enough skilled cybersecurity professionals.

Accomplishments and Initiatives to Leverage

1. **Build upon the Following Successful Private and Public Sector Partnerships**
   a. The Financial Services Sector Coordinating Council (FSSCC) consists of private sector owners, operators, utilities and trade associations, representing a cross-section of the financial services industry. It partners with the financial services government coordinating council – the Financial and Banking Information Infrastructure Committee (FBIIC) – to address critical infrastructure policy issues and strengthen industry resiliency and preparedness.
   b. The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established in 1999 and brings together 7,000 financial services companies to share globally tactical and operational information and insights.
   c. The Joint Financial Associations Cybersecurity Summits was established in 2013 and brings financial sector and government executives together twice each year to discuss, coordinate and collaboration on sector resiliency, cyber threats, and capability gaps.
   d. The Financial Systemic Resilience and Analysis Center (FSARC) was established in 2016 by financial service firms that the US Government has designated as "critical infrastructure" entities. The mission of the FSARC is to proactively identify, assess, and coordinate efforts to mitigate systemic risk from cyber security threats.
2. **Leverage Cybersecurity Act of 2015 to Encourage Information Sharing**
   a. Enhance private-public sector collaboration that results in increased information sharing in a timely, trusted, and actionable manner and leverages the liability and anti-trust protections embodied in the Cybersecurity Act of 2015.
3. **Presidential Policy Directive 41, United States Cyber Incident Coordination**
   a. Continued private-public collaboration is required to develop the list of cyber defense capabilities that can be used to respond to a significant cyber incident affecting the nation's critical infrastructure.

Sincerely,

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

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr.
Suite 230
Reston, VA 20191

Appendix: Key Financial Sector Cyber Accomplishments and Initiatives

The U.S. financial services sector has worked diligently over the past two decades to enhance cyber defenses in collaboration with U.S. Government agencies and other critical infrastructure sectors. The following are key financial sector cyber accomplishments and initiatives:

- Established the ***Financial Services Information Sharing and Analysis Center (FS-ISAC)*** in 1999 to facilitate information sharing and analysis of cyber and physical threats facing the financial services sector. Today, the FS-ISAC has about 7,000 member financial institutions and trade associations in 38 countries.

- Established the ***Financial Services Sector Coordinating Council (FSSCC)*** in 2002 to coordinate the development of critical infrastructure strategies and initiatives with its financial services members, trade associations, and other industry sectors. The FSSCC has built and maintained relationships with the Federal Government's Financial and Banking Information Infrastructure Committee (FBIIC), which serves as the Government Coordinating Council for the Financial Services Sector and includes the U.S. Department of Treasury (Treasury) and Department of Homeland Security (DHS), all the federal financial regulatory agencies, and law enforcement agencies.

- Developed and convened 13 **"Hamilton Series"** cyber exercises in 2014-16 in collaboration with the various U.S. Government agencies to better prepare the financial sector in addressing the risks and challenges presented by significant cybersecurity incidents. The exercises ranged from regionally-focused events among small and medium sized companies to exercises at the U.S. Treasury Department and Federal Reserve Bank of New York involving large, systemically important financial sector companies. Additionally, these scenarios examined impacts to different segments of the financial sector, including impacts to equities markets, large, regional, and medium-sized depository institutions, payments systems and liquidity, and futures exchanges.

- Coordinated extensively with Treasury, DHS, and the White House on the development of ***Presidential Policy Directive (PPD) 41***, July 2016, which outlines the U.S. Government's response protocols for a cyber security incident.

- Improved and expanded ***cross-sector and public-private information sharing and collaboration,*** *including* providing subject matter expertise and advocacy to support the **Cybersecurity Act of 2015**; investing in technologies and standards to automate cyber threat/attack information sharing; embedding a financial sector expert in DHS's National Cybersecurity and Communications Integration Center; expanding membership in the FS-ISAC and working with the Electricity Subsector and Communications Sector to foster integrated responses to cybersecurity.

- ***Fostered sector-wide cybersecurity collaboration*** through eight **Joint Financial Associations Cybersecurity Summits**. Since 2013, the Summits have brought together key financial sector and government executives to discuss Sector resiliency, address cyber threats and capability gaps, and enhance coordination and collaboration.

- Created ***Sheltered Harbor*** to enhance resiliency and provide augmented protections for financial institutions' customer accounts and data. The focus of Sheltered Harbor is to extend the industry's capabilities to securely store and restore account data, should the need arise. Sheltered Harbor is an additional layer of protection on top of existing defenses that many financial firms utilize. It is one of a series of proactive initiatives undertaken by the U.S. financial services industry to improve sector-wide resilience. The concept for Sheltered Harbor

Financial Services Sector Coordinating Council
12020 Sunrise Valley Dr.
Suite 230
Reston, VA 20191

arose during a series of successful cybersecurity simulation exercises between public and private sectors and known as the "Hamilton Series."

- Created the ***Financial Systemic Resilience and Analysis Center (FSARC)***, a subsidiary of the FS-ISAC. The mission of the FSARC is to proactively identify, assess, and coordinate efforts to mitigate systemic risk from cyber security threats. FSARC membership is limited to those entities within the financial sector designated as "critical infrastructure" under Executive Order 13636 (February 2013).
- Updated and tested ***cyber response plans***, including the All-Hazards Crisis Response Playbook, to assign responsibilities for collaboration, communication, and decision-making within the financial sector and key partners in other sectors and the Federal Government.