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

Testimony of

Gregory T. Garcia

On Behalf of the

Financial Services Sector Coordinating Council

On

"Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"

Before the

U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

May 19, 2015

Chairman Neugebauer, Ranking Member Clay, and Members of the Subcommittee, thank you for this opportunity to address the Subcommittee about how the financial sector addresses cyber threats.

My name is Greg Garcia. I am the Executive Director of the Financial Services Sector Coordinating Council (FSSCC). Established in 2002, FSSCC involves 65 of the largest financial firms and industry associations representing clearinghouses, commercial banks, credit card networks; credit rating agencies; exchanges; electronic communication networks; financial advisory services; insurance companies; financial utilities; government-sponsored enterprises; investment banks; merchant and retail banks; and electronic payment firms. This community shares responsibility and commitment to the protection of our sector that is commensurate with their substantial importance to the resilience of the national and global economy.

The FSSCC was established in accordance with the critical infrastructure protection framework promulgated first in Presidential Decision Directive (PDD) 63 in 1998, which was superseded in 2003 by Homeland Security Presidential Directive 7 and in 2013 by Presidential Policy Directive 21.

As with many industry associations, its governing structure includes a rotating chairmanship and an executive committee, with numerous outcome-oriented working groups focused on specific deliverables to achieve the organization's objectives. The current chairman, serving the first year of his two year term, is Russell Fitzgibbons, the Chief Risk Officer and Executive Vice President of The Clearing House.

Today I will discuss an overview of the cyber threats faced by the financial sector, and how it is organized under regulatory and partnership frameworks to manage cyber risk.

PROFILE OF THE FINANCIAL SECTOR AND ITS STATUS AS CRITICAL INFRASTRUCTURE

Congress and the Administration have defined "critical infrastructure" as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

Section 9 of Executive Order 13636, issued in 2013 requires that DHS identify critical infrastructure against which a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security. The primary purpose of this process is to improve understanding of national and regional cyber dependencies and consequences across critical infrastructure, inform planning and program development for federal critical infrastructure security and resilience programs, and motivate identified critical infrastructure owners and operators to maintain robust cyber risk management programs.

Collectively, the organizations that make up the financial services sector are connected through a network of electronic systems with many entry points, and most of the sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity of paramount importance to the sector. A successful cybersecurity or physical attack on these systems could have significant impacts on the global economy and the nation.

For example, malicious cyber actors with increasing sophistication and persistence continue to target the financial services sector. These actors vary considerably in terms of motivation and capability, from nation states conducting corporate espionage to advanced cyber criminals seeking to steal money, to hacktivists intent on making political statements. Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems, even inadvertently.

In order to maintain a strong risk management partnership against potential high-impact cyber events, the Treasury Department, financial regulators, the Department of Homeland Security, and law enforcement and other government partners coordinate regularly with financial institutions to identify critical systems, infrastructure, operations and institutions, as well as current and emerging threats to those systems, in order to develop appropriate security and resilience strategies.

FSSCC MISSION

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. During the past decade, this strategic partnership has continued to grow, in terms of the size and commitment of its membership and the breadth of issues it addresses.

In simplest terms, members of the FSSCC assess security and resiliency trends and policy developments affecting our critical financial infrastructure, and coordinate among ourselves and with our partners in government and other sectors to develop a consolidated point of view and coherent strategy for dealing with those issues.

Accordingly, our sector's primary objectives are to:

- Implement and maintain structured routines for sharing timely and actionable information related to cyber and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.
- Improve risk management capabilities and the security posture of firms across the financial sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.
- Collaborate with homeland security, law enforcement and intelligence communities, financial regulatory authorities, other industry sectors, and international partners to respond to and recover from significant incidents.
- Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

We have learned that a strong risk management strategy for cyber and physical protection involves participating in communities of trust that share information about threats, vulnerabilities, and incidents affecting those communities. That strategy is based on the simple concepts of strength in numbers, the neighborhood watch, and shared situational awareness.

To achieve this goal, public and private sector partners exchange data and contextual information about specific incidents and longer term trends and developments. Sharing this information helps to prevent

incidents from occurring and to reduce the risk of a successful incident at one firm later impacting another. These efforts increasingly focus on including smaller firms and include international partners.

Together we are undertaking or have accomplished numerous initiatives to:

- Improve information sharing content and procedures between government and the sector;
- Conduct joint exercises to test our communications, response and resiliency protocols during incident scenarios affecting different segments of the financial system;
- Maintain an "All Hazards Crisis Response Playbook" and within it a "Cyber Response Coordination Guide" that leads incident responders and executive decision makers through decision and action processes based on identified impacts and severity of incidents;
- Prioritize critical infrastructure protection research and development (R&D) funding needs
- Engage with other critical sectors and international partners to understand and leverage our interdependencies;
- Advocate broad adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, including among small and mid-sized financial institutions across the country;
- Develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies; and
- Create financial services sector-owned, operated and governed .BANK and .INSURANCE top-level internet domains. The .BANK and .INSURANCE domains have robust operational standards including: eligibility requirements; verification; name selection standards; and security-focused technical requirements such as Domain Name System Security Extensions (DNSSEC); encryption standards; email authentication requirements designed to reduce phishing and spoofing activities; and more.

At the same time, understanding the sector's dependencies on the delivery of services from other key sectors such as communications, energy and information technology is necessary for better understanding threats and assuring rapid recovery and business continuity planning against disruption of critical financial functions, regardless of the cause.

FS-ISAC INFORMATION SHARING PROGRAMS AND OPERATIONS

For the financial sector, the primary community of trust for critical financial infrastructure protection is the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is the tactical and operational member organization that informs the FSSCC's strategic policy mission.

The FS-ISAC was formed in 1999 in response to the 1998 PDD 63, which called for the public and private sectors to work together to address physical and cyber threats to the nation's critical infrastructures. This role was reinforced after 9/11 and continues to strengthen to address evolving threats to critical infrastructure.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were 68 members, primarily larger financial services firms. Since that time, the membership has expanded to more than 5000 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, data security payments processors, and 24

trade associations representing virtually all of the U.S. financial services sector. Most recently, there has been a significant increase in the number of small and medium sized entities that have joined FS-ISAC.

Since its founding, the FS-ISAC's operations and culture of trusted collaboration have evolved into what we believe is a successful model for how other industry sectors can organize themselves around this security imperative. The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that facilitates sharing of actionable threat, vulnerability and incident information in a non-attributable and trusted manner among members, the sector, and its industry and government partners, ultimately benefiting the nation.

FS-ISAC information sharing activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
- An anonymous online submission capability to facilitate member sharing of threat, vulnerability, incident information and best practices in a non-attributable and trusted manner;
- Support for attributable threat information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, and the Payments Risk Council;
- Bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- Emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS); and
- Participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for FSSCC exercises such as the Hamilton series, CyberFIRE and Quantum Dawn.

FINANCIAL SECTOR PARTNERSHIPS

The financial sector works closely with various government agencies including the Department of Treasury, which leads the Finance and Banking Information Infrastructure Committee (FBIIC); DHS; Federal Financial Institutions Examination Council (FFIEC) regulatory agencies; United States Secret Service; Federal Bureau of Investigation (FBI); the intelligence community; and state and local governments.

In addition to our close working relationship with the Treasury Department and financial regulatory agencies, financial sector stakeholders participate in a variety of strategic and information sharing programs operated by DHS. For example:

- The financial sector and Treasury Department maintain a physical presence, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, within the DHS National Cybersecurity and Communications Integration Center (NCCIC), which serves as a hub for sharing information related to cybersecurity and communications incidents across sectors, among other roles and responsibilities.
- Supplementing our information sharing engagement within NCCIC is the DHS Cyber Information Sharing and Collaboration Program (CISCP) which enables collaborative threat analysis between

industry and government in an operational and trusted environment that speeds time to response.

- Also useful to the financial sector, particularly smaller community institutions, is the Critical Infrastructure Cyber Community (C^3, or "C-Cubed") Voluntary Program, which supplements the NIST Cyber Security Framework, and provides guidance on how institutions can improve their cyber risk management programs, regardless of size and sophistication.
- The Office of Cyber & Infrastructure Analysis helps critical sectors evaluate cross sector interdependencies with risk and threat assessments, and is currently undertaking an interdependency assessment between financial services and telecommunications infrastructure in the Chicago area.
- The financial sector has developed an R&D agenda highlighting the priority R&D initiatives we believe will enhance protection of our critical financial infrastructure, and we have consulted with the DHS Science and Technology Directorate to help inform their funding priorities.
- The sector also works closely with the National Infrastructure Coordinating Center (NICC), the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government.
- Most recently, the financial sector has begun planning and executing a series of sector-wide cyber exercises that test our ability to share information and respond to critical incidents collaboratively with our government partners. The DHS NCCIC management and operations team has been an important partner in this process, as have the Treasury Department and other key government stakeholders, lending their expertise and resources toward developing the scenarios and supporting the execution and after-action reports of the exercises.
- Through the promulgation of DHS-funded open specifications for automated threat information sharing, the FS-ISAC has developed a capability that is widely used by the financial sector and other sectors. Known as Soltra Edge, this tool automates threat sharing and analysis and speeds time to decision and mitigation from days to hours and minutes.
- Finally, the FS-ISAC and FSSCC have worked closely with government partners to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided useful information for the sector to implement effective risk controls to combat these threats.

AUTOMATED THREAT INFORMATION SHARING

The sector continues to make significant progress toward increasing the speed and reliability of its information sharing efforts through expanded use of DHS-funded open specifications, including Structured Threat Information eXchange (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™).

Late last year, the financial sector announced the "Soltra Edge" automated threat capability, which is the result of a joint venture of the FS-ISAC and the Depository Trust and Clearing Corporation (DTCC). This capability addresses a fundamental challenge in our information sharing environment: typically the time associated with chasing down any specific threat indicator is substantial. The challenge has been to help our industry increase the speed, scale and accuracy of information sharing and accelerate time to resolution.

The Soltra Edge tool reduces a huge burden of work for both large and small financial organizations, including those that rely on third parties for monitoring and incident response. It is designed for use by many parts of the critical infrastructure ecosystem, including the financial services sector; the healthcare sector; the energy sectors; transportation sectors; other ISACs; national and regional CERTs (Computer Emergency Response Teams); and vendors and services providers that serve these sectors.

Key goals of Soltra-Edge are to:

- Deliver an industry-created utility to automate threat intelligence sharing
- Reduce response time from days/weeks/months to seconds/minutes
- Deliver 10 times reduction in effort and cost to respond
- Operate on an at-cost model over open standards (STIX, TAXII)
- Leverage DTCC scalability; FS-ISAC community and best practices
- Provide a platform that can be extended to all sizes of financial services firms, other ISACs and industries
- Enable integration with vendor solutions (firewalls, intrusion detection, anti-virus, threat intelligence, etc.)

With these advancements, one organization's incident becomes everyone's defense at machine speed. We expect this automated solution to be a "go-to" resource to speed incident response across thousands of organizations in many countries within the next few years.

REGULATORY INTERESTS

The financial sector is often credited for having developed a "mature" cyber security risk management posture. This is due in part to the fact that financial services is a heavily regulated industry, and also to the overarching imperative that our business models, consumer confidence and the stability of the financial system and the global economy are dependent upon a secure and resilient infrastructure.

As just one example, Title V of the Gramm-Leach-Bliley Act (GLBA) requires banks to develop and maintain an information security program, and implement a "risk-based" response program to address instances of unauthorized access to customer information systems.

At a minimum, a response program must:

- Assess the nature and scope of any security incident and identify what customer information systems and customer information may have been accessed or misused;
- Notify the institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information."
- Notify appropriate law enforcement authorities and file Suspicious Activity Reports in situations involving federal criminal violations requiring immediate attention;
- Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information, and
- Notify customers "as soon as possible" if it is determined that misuse of customer information has occurred or is reasonably possible. Where appropriate, the notice also must include:
    - Recommendation to review account statements immediately and report suspicious activity;

- Description of fraud alerts and how to place them;
- Recommendation that the customer periodically obtain credit reports and have fraudulent information removed;
- Explanation of how to receive a free credit report; and
- Information about the FTC's identity theft guidance for consumers.

More broadly, financial sector institutions comply with varying cybersecurity requirements and guidance from many regulatory bodies:

- The Securities and Exchange Commission (SEC)
- Financial Industry Regulatory Authority (FINRA)
- The Federal Reserve System
- The Office of the Comptroller of the Currency (OCC)
- The Federal Deposit Insurance Corporation (FDIC)
- The Consumer Financial Protection Bureau (CFPB)
- The U.S. Commodity Futures Trading Commission (CFTC)
- State banking agencies
- State insurance agencies

The financial sector supports the need for regulatory guidance on effective standards of practice for cybersecurity risk management. It's a constantly moving target, and just as financial institutions need to regularly calibrate their controls to evolving threats, so do the regulatory agencies need to keep pace with new threats, new financial business process models and the necessary skill sets to evaluate the intersection of those two for security and resiliency purposes.

But as the regulatory agencies are independent, there is not sufficient coordination among them to ensure we are all aligned with unity of effort toward a common objective: financial services security and resiliency. Perhaps because of this, we have seen examples of agencies each asking their own set of cybersecurity examination questions. As a sector we would urge more uniformity among the regulatory agencies in their examination procedures and in the range of questions they ask. This process could be more efficient to allow financial institutions to focus more on securing our infrastructure and less on answering multiple questionnaires in different ways. And we are looking forward to seeing how agencies will or will not map their examination standards to the NIST Cybersecurity Framework. The Framework is an exemplary industry-government collaboration that involved extensive time, effort and resources in the development of guidance for tailored and scalable cybersecurity risk management.

Mr. Chairman and Members of the Committee, this concludes my testimony.