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

"From Protection to Partnership: Funding the DHS Role in Cybersecurity."

Before the

United States Senate
Committee on Appropriations
Subcommittee on Homeland Security

April 15, 2015

Chairman Hoeven, Ranking Member Shaheen, and Members of the Subcommittee, thank you for this opportunity to address the Subcommittee about funding the DHS role in cybersecurity and its partnership with the private sector.

My name is Gregory T. Garcia. I am the Executive Director of the Financial Services Sector Coordinating Council (FSSCC), which was established in 2002 and involves 65 of the largest financial services providers and industry associations representing clearinghouses, commercial banks, credit card networks and credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms.

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critical infrastructure protection framework promulgated first in Presidential Decision Directive 63 in 1998, which was superseded in 2003 by Homeland Security Presidential Directive 7 and in 2013 by Presidential Policy Directive 21.

FSSCC membership includes critical financial enterprises and their industry associations whose responsibility and commitment to the protection of our sector is commensurate with their substantial importance to the resilience of the national and global economy.

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.

What I will cover today is an overview of the financial sector's tactical and strategic components, and how we manage cyber risk with the Department of Homeland Security, the Treasury Department, and other key government and industry partners.

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:

1. 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.
2. 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.
3. 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.
4. Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

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

Accordingly, we partner with the Department of Treasury as our sector specific agency, the Department of Homeland Security, law enforcement, the intelligence community, other critical sectors, and financial regulatory agencies forming our Government Coordinating Council counterpart – called the Financial and Banking Information Infrastructure Committee (FBIIC).

Together we are undertaking numerous initiatives to:

- Improve Information sharing content and procedures between government and the sector;
- Conduct joint exercises to test our resiliency and information sharing procedures under differing scenarios;
- Prioritize critical infrastructure protection research and development funding needs
- Engage with other critical sectors and international partners to better understand and leverage our interdependencies;
- Advocate broad adoption of the NIST Cybersecurity Framework, including among small and mid-sized financial institutions across the country; and
- Develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies.

FINANCIAL SECTOR PARTNERSHIP WITH THE DEPARTMENT OF HOMELAND SECURITY

Of particular relevance to the topic of this hearing, financial sector stakeholders participate in a variety of strategic and information sharing programs operated by the Department of Homeland Security. For example:

- The financial sector and Treasury Department maintain a physical presence 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 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 a research and development (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 Financial Services Information Sharing and Analysis Center (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. I will discuss FS-ISAC activities in more detail below.

In sum, the financial sector has been able to benefit substantially from its close information sharing relationship with DHS.

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 organization that informs the FSSCC's strategic policy mission.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (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 in response to Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act.

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, mostly 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.

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 provides anonymity to allow members to share threat, vulnerability and incident information in a non-attributable and trusted manner. The FS-ISAC provides a formal structure for valuable and actionable information to be shared among members, the sector, and its industry and government partners, which ultimately benefits 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 information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, threat intelligence sharing open to the membership, 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.

FS-ISAC PARTNERSHIPS

The FS-ISAC works closely with various government agencies including the Department of Treasury, DHS, Federal Reserve, 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 partnership with DHS, FS-ISAC two years ago became the third ISAC to have representation on e the NCCIC watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government, as well as other critical sectors, and there are numerous examples of success to illustrate this.

As part of this partnership, the FS-ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in near real-time. This listserv allows FS-ISAC members to share directly with U.S. CERT and further facilitates the information sharing that is already occurring between FS-ISAC members and with the NCCIC watch floor or with other government organizations.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG) and the group has been actively engaged in incident response. The Cyber UCG's handling and communications with various sectors following the distributed denial of service (DDOS) attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.

Finally, the FS-ISAC and FSSCC have worked closely with its 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 a new automated threat capability it created called "Soltra Edge", 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 capability developed by the sector removes 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 the tenets of at-cost model and open standards (STIX, TAXII)
- Leverage DTCC scalability; FS-ISAC community & 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.

IMPORTANCE OF DHS FUNDING AND STRONG OVERSIGHT FOR IMPROVED PARTNERSHIP

DHS is currently responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure – a critical and expansive mission. In the realm of information sharing, DHS's role could expand further with increased information sharing following the implementation of the President's February 13, 2015 Executive Order to promote private sector information sharing. Should Congress enact legislation establishing a streamlined voluntary information sharing legal framework, DHS will likely receive additional information from private sector partners on cyber threats. This will increase the already existing need for a robust analytic capability at DHS to develop products, particularly at the unclassified level, that will be useful and actionable to its domestic and international stakeholder community, both inside and outside the government.

It is critical that DHS have the necessary personnel and technical tools to enable them to complete their mission. Last year, Congress passed additional personnel authorities for DHS to hire trained, qualified personnel to work in cybersecurity positions, which will hopefully make the recruitment and retention of qualified personnel more successful.

In this era of fiscal restraint, we also appreciate the need to ensure that appropriated funds are being spent in the most effective and efficient manner. We believe this is a role not only for senior DHS management, but Congress as well, as the ultimate appropriators of funding. This can strengthen DHS's cyber programs and provide sector stakeholders better information with which to defend their own networks and ultimately strengthen the security of our nation's infrastructure.

Overall, our assessment is that the financial sector's relationship with DHS is productive and directionally positive, with tangible successes that we believe are improving the protection and resilience of our critical financial infrastructure. Where there are programmatic gaps or implementation inefficiencies in the partnership, they are mutually acknowledged and addressed. Ultimately, we recognize that as our joint effort matures over time, we are never done, only better.

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