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

Industry Perspectives on the President's
Cybersecurity Information Sharing Proposal

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and
Security Technologies

March 4, 2015

Chairman Ratcliffe, Ranking Member Richmond, and members of the Subcommittee, thank you for this opportunity to address the Subcommittee about the President's information sharing executive order.

My name is Gregory T. Garcia. I am 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.

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's economic security. During the past decade, this strategic partnership has continued to grow, in terms of both the size and commitment of its membership and the breadth of issues it addresses. Members volunteer their time and resources to FSSCC with a sense of responsibility to the broader sector, financial consumers and the nation.

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 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 sectors of industry, 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.

To achieve these objectives we partner with the Department of Treasury, DHS, law enforcement, and financial regulatory agencies forming our Government Coordinating Council counterpart – called the Financial and Banking Information Infrastructure Committee (FBIIC).

Rolling up into those broad objectives are numerous initiatives undertaken collaboratively within this public-private partnership, including committee-organized workstreams to, for example:

- 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
- develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies.

We have learned over the years that a foundational element of any strong risk management strategy for cyber and physical protection involves participation 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.

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.

Financial sector stakeholders participate in information sharing programs operated by the Department of Homeland Security. For example, the financial sector and Treasury Department maintain a presence within the 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. The sector also works closely with the National Infrastructure Coordinating Center (NICC), which is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government.

The financial sector benefits greatly from its close information sharing relationship with law enforcement partners, including the Federal Bureau of Investigations and the United States Secret Service.

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 operational heartbeat of the FSSCC strategic body.

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 cyber threats to the nation's critical infrastructures. 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 expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, 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 amongst 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 and incident information in a non-attributable and trusted manner;

- operation of email listservs supporting attributable information exchange by various special interest groups including the Financial Services Sector Coordinating Council (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;

- anonymous surveys that allow members to request information regarding security best practices at other organizations;
- 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);
- emergency conference calls to share information with the membership and solicit input and collaboration;
- engagement with private security companies to identify threat information of relevance to the membership and the sector;
- participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for FSSCC exercises such as CyberFIRE and Quantum Dawn
- development of risk mitigation best practices, threat viewpoints and toolkits, and preparation of cyber security briefings and white papers;
- administration of Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee, which: provide in-depth analyses of risks to the sector, conduct technical, business and operational impact assessments; determine the sector's cyber and physical threat level; and, recommend mitigation and remediation strategies and tactics;
- special projects to address specific risk issues such as the Account Takeover Task Force
- document repositories for members to share information and documentation with other members;
- development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;
- semi-annual member meetings and conferences; and

- online webinar presentations and regional outreach programs to educate organizations, including small to medium sized regional financial services firms, on threats, risks and best practices.

FS-ISAC PARTNERSHIPS

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (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 participate in the National Cybersecurity and Communications Integration Center (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 Data 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, 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). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. 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.

Consistent with the directives of Presidential Policy Directive 21 and Executive Order 13636 of 2014, the Treasury established the Cyber Intelligence Group (CIG) as part of the Office of Critical Infrastructure Protection and Compliance Policy. The CIG was established in response to a need identified by the financial sector for the government to have a focal point for sharing cyber threat-related information with the sector. The CIG identifies and analyzes all-source intelligence on cyber threats to the financial sector; shares timely, actionable information that alerts the sector to threats and enables firms' prevention and mitigation efforts; and solicits feedback and information requirements from the sector.

Finally, it should be noted that 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.

In addition, several membership subgroups meet regularly with their own circles of trust to share information, including: the Insurance Risk Council (IRC); the Community Institution Council (CIC) with hundreds of members from community banks and credit unions; and the Community Institution Toolkit Working Group with a mission to develop a framework and series of best practices to protect community institutions. This includes a mentoring program to assist community institutions just getting started with an IT security staff.

The FS-ISAC also works very closely with the other critical infrastructure sectors on an ISAC to ISAC basis as well as through the National Council of ISACs. Information about threats, incidents and best practices is shared daily among the ISACs via ISAC analyst calls, and a cross-sector information sharing platform. The ISACs also come together during a crisis to coordinate information and mitigations as applicable.

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. 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.

EXERCISES

The sector regularly tests its resilience through exercises to identify gaps and exercise processes related to information sharing. Efforts such as the annual "Cyber Attack against Payment Processes (CAPP)", "Quantum Dawn" and public/private exercises provide essential insight into our ability individually and collaboratively to respond to various attack scenarios.

In carrying out this information sharing partnership, the financial sector and government partners are committed to ensuring that individual privacy and civil liberties protections are incorporated into all activities, to include technical analysis, information sharing on threats, and incident response efforts.

THE PRESIDENT'S EXECUTIVE ORDER ON PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

As discussed above, the Financial Services Sector Coordinating Council (FSSCC) considers strong collaboration and information sharing within the sector and with government to be a critical element of cybersecurity risk management.

Thus, in alignment with the FS-ISAC's statement for the record by Denise Anderson, vice president of the FS-ISAC and Chair of the National Council of ISACs, we applaud this Administration's efforts to improve our cybersecurity information sharing environment so that we can better anticipate, protect against and respond to cyber threats. The Administration's executive action is a positive step toward increasing the volume and quality of actionable and timely cybersecurity information.

With key federal support from the Treasury Department as our Sector Specific Agency, law enforcement and the Department of Homeland Security (DHS), our network defenders are better able to prepare for

cyber threats when there is a consistent, reliable and sustainable flow of actionable cybersecurity information and analysis, at both a classified and unclassified level.

We are making some progress toward this goal, but it has become increasingly necessary for appropriately-cleared representatives of critical sectors such as financial services to have access, and provide contributions, to classified information that enables analysts and operators to take timely action to defend essential systems. Accordingly, the executive order's enhancement of DHS's role in accelerating the security clearance process for critical sector owners and operators is a clear indication of the Administration's support for this public-private partnership.

In considering enhancements to this model, agility and innovation are essential for the operational resilience of critical sector functions. In this spirit, we support the creation of Information Sharing and Analysis Organizations (ISAOs) as a mechanism for all sectors, regions and other stakeholder groups to share cybersecurity information and coordinate analysis and response.

While ISACs must retain their status as the government's primary critical infrastructure partners given their mandate for broad sectoral representation, the development of ISAOs should be facilitated for stakeholder groups that require a collaborative cyber and physical threat information sharing capability that builds on the strong foundation laid by the ISACs.

As the ISAO standards development process unfolds, the FSSCC believes certain principles must be upheld for structuring both the ISAOs themselves and the government's interaction with them:

- Sharing of sensitive security information within and among communities of trust is successful when operational standards of practice establish clear and enforced information handling rules.
- Information sharing is not a competitive sport: while competition in innovation can improve technical capabilities, operational standards should incentivize federated information sharing. Threat and vulnerability intelligence needs to be fused across trust communities, not diffused or siloed.
- Government internal processes for collecting, analyzing and packaging CIP intelligence for ISAC/ISAO consumption must be streamlined and transparent to maximize timeliness, accuracy and relevance of actionable shared information. Indeed, Section 4 of EO 13636 directs the government to improve its dissemination of cyber threat intelligence to the private sector, enabling entities to protect their networks. Full implementation of this directive is necessary to achieve the objectives of the President's information sharing executive order.
- To manage scarce resources, government information sharing mechanisms such as the National Cyber and Communications Integration Center (NCCIC) and the Treasury Department's Cyber Intelligence Group (CIG) should prioritize engagements with ISACs and ISAOs according to transparently established impact criteria, such as government capacity to effectively serve CIP constituents in steady-state and surge mode, the reach those CIP stakeholders have into their sectors, and the effectiveness of their capabilities.

It is also important that the process to develop the ISAO standards is collaborative, open, and transparent. The process managed by the National Institute of Standards and Technology (NIST) during the development of the NIST Cybersecurity Framework is an excellent example of the appropriate leveraging of private sector input, knowledge and experience to develop guidance that will primarily impact non-governmental entities. We encourage DHS, as the implementing authority of the

president's EO, to emulate the engagement model that NIST used to create and adopt their Cybersecurity Framework. The process worked.

Finally, for DHS to be successful implementing this EO and its many cyber security risk management and partnership authorities, it must be sufficiently resourced with the best analytical and technical capabilities, with a cadre of highly qualified cybersecurity leaders and analytical teams to conduct its mission. There must be a concerted effort to recruit, retain and maintain a world class workforce that is able to assess cyber threats globally and help the private sector reduce risk to this nation.

The FSSCC believes that, with the application of the principles discussed in this statement, the creation of ISAOs and their partnership agreements with DHS have the potential to complement the ISAC foundation and measurably improve cyber risk reduction for critical infrastructure and the national economy.

On the subject of legislation, Mr. Chairman, passing cyber threat information sharing legislation that encourages more information sharing between the private sector and government and within the private sector, with fewer concerns about liability, will have a positive operational impact on the security of the nation's networks. This sector-wide position is articulated in detail in recent letters from leading financial services trade associations.

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