



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

*Written Statement of*

Jane Carlin

Chairperson

*On behalf of the*

Financial Services Sector Coordinating Council  
(FSSCC)

*Before the*

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

*On*

The Department of Homeland Cybersecurity Mission: Promoting Innovation and Securing  
Critical Infrastructure

April 15, 2011

Written Statement of Jane Carlin, FSSCC Chairperson  
April 15, 2011

Chairman King, Subcommittee Chairman Lungren, Ranking Member Thompson and members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Homeland Security Committee, I am Jane Carlin. I serve as the chairperson of Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (“FSSCC”). I also am the Managing Director and Global Head of Operational Risk, Business Continuity, Information Security, and Risk and Insurance Management at Morgan Stanley.

Thank you for inviting me to testify on behalf of the Financial Services Sector Coordinating Council for Homeland Security and Critical Infrastructure Protection (“FSSCC”) on the Department of Homeland Security Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure. My testimony today will address the following: background information on the FSSCC, engagement with DHS, lessons learned from recent cyber attacks, recommendations for improving public-private partnership, and comments on cybersecurity legislation.

### **Background on FSSCC and Public-Private Partnership**

The FSSCC was established in 2002 in response to the September 11, 2001 attacks and at the request of the U.S. Treasury Department in harmony with Presidential Decision Directive 63 of 1998. Presidential Decision Directive 63 required sector-specific federal departments and agencies to identify, prioritize, and protect United States critical infrastructure and key resources and to establish partnerships with the private sector.

The FSSCC has 52 member associations and financial institutions representing clearinghouses, commercial banks, 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.<sup>1</sup> FSSCC members dedicate a significant amount of time and resources to this partnership for critical infrastructure protection and homeland security. The FSSCC does not collect dues and its success as a volunteer organization relies heavily on the time members contribute and to the expertise and leadership roles members play within their respective financial institutions and associations. Appendix A includes the current FSSCC organizational chart, including those who serve in leadership roles of seven

---

<sup>1</sup> Members including: American Bankers Association, American Council of Life Insurers, American Insurance Association, American Society for Industrial Security International, BAI, Bank of America, Bank of NY/Mellon, Barclays, BITS/The Financial Services Roundtable, CME Group, ChicagoFIRST, Citigroup, The Clearing House, CLS Group, Consumer Bankers Association, Credit Union National Association, The Depository Trust & Clearing Corporation, Fannie Mae, Financial Industry Regulatory Authority, Financial Information Forum, Financial Services Information Sharing and Analysis Center, Freddie Mac, Futures Industry Association, Goldman Sachs, ICE Futures U.S., Independent Community Bankers of America, Investment Company Institute, JP Morgan Chase, Managed Funds Association, Morgan Stanley, NACHA — The Electronic Payments Association, The NASDAQ Stock Market, Inc., National Armored Car Association, National Association of Federal Credit Unions, National Futures Association, Navy Federal Credit Union, NYSE Euronext, The Options Clearing Corporation, Securities Industry and Financial Markets Association, State Farm, State Street Global Advisors, Travelers, VISA USA Inc.

committees that address crisis event management, cross sector coordination, cybersecurity, international, long-range vision, policy and research and development.

On August 3, 2010, I was selected by members of the FSSCC to serve as the chairperson. I am preceded by four FSSCC chairpersons: Shawn Johnson of State Street Global Advisors (SSGA) from 2008-10, George Hender of the Options Clearing Corporation (OCC) from 2006-08, Don Donahue of Depository Trust and Clearing Corporation (DTCC) from 2004-06, and Rhonda MacLean of Bank of America from 2002-04. Prior to my selection, I served as FSSCC's vice chairperson and head of the FSSCC Cybersecurity Committee from June 2008 to August 2010. Additionally, I serve on the Executive Committee and Board of the Partnership for Critical Infrastructure Security (PCIS), which is the private sector organization that coordinates homeland security issues for all national critical infrastructure sectors.

Each year the FSSCC submits an annual report on our activities. This annual report is published by the Department of Homeland Security along with reports from the other CIP sectors. Appendix B is the executive summary of our most recent Sector Annual Report which provides an overview of our role and activities. Our partnership is frequently heralded as the model and aspired to by the other 17 critical infrastructure sectors.

The goal of the FSSCC is to continue to improve the resilience and availability of financial services by working through its public-private partnership to address the evolving nature of threats and vulnerabilities and the risks posed by the sector's dependence on other critical sectors. In support of this goal, the FSSCC established four objectives in 2010:

- Identify threats and promote protection
- Drive preparedness
- Collaborate with the Federal government
- Coordinate crisis response

In support of these objectives the FSSCC's current priorities include:

- Information sharing
- Crisis event management
- Threat matrix dissemination and management
- Communication and outreach
- Identity assurance

In 2002, the Treasury Department also chartered the Financial and Banking Information Infrastructure Committee (FBIIC) under the President's Working Group on Financial Markets.<sup>2</sup> The FBIIC is charged with improving coordination and communication among

---

<sup>2</sup> The FBIIC was organized under Executive Order 13231 of October 16, 2001 entitled *Critical Infrastructure Protection in the Information Age*. Members of the FBIIC include: American Council of State Savings Supervisors; Commodity Futures Trading Commission; Conference of State Bank Supervisors; Department of the Treasury; Farm Credit Administration; Federal Deposit Insurance Corporation; Federal Housing Finance Agency; Federal Reserve Bank of New York; Federal Reserve Board; National Association of Insurance Commissioners; National Association of State Credit Union Supervisors; National Credit Union Administration; North American Securities Administrators Association; Office of the Comptroller of the Currency; Office of Thrift Supervision; Securities and Exchange Commission; and Securities Investor Protection Corporation.

financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. The U.S. Department of the Treasury serves as the Sector Specific Agency (SSA) for the Banking and Finance Sector. The FSSCC-FBIIC public-private partnership was confirmed in Homeland Security Presidential Directive 7 of 2003.

The FSSCC and FBIIC meet jointly at least three times a year, supplemented by monthly conference calls. Earlier this week, over 80 executives, experts and officials from the FSSCC and FBIIC met in Chicago to discuss a wide range of issues, including: information sharing, regional coalitions, threats, and cyber incident reviews.

In addition to the collaboration with the FBIIC, it is important to remind the committee that the financial services sector is highly regulated by international, Federal and state authorities. Through numerous laws enacted by Congress over the past 150 years, federal financial regulators have implemented a complex regime that includes supervision of the financial institutions' operational, financial and technological systems. Regulators, such as the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Securities and Exchange Commission, conduct examinations to assess the adequacy of controls to address financial and other risks. These examinations focus on information security, business continuity, vendor management and other operational risks. In addition to these public sector entities, self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), the National Futures Association (NFA), and exchanges, such as the Chicago Mercantile Exchange (CME), and the New York Stock Exchange (NYSE), also play an important role in industry oversight.

### **Engagement with DHS**

The FSSCC has a productive and expanding relationship with the Department of Homeland Security (DHS), but more is needed. Our engagement with DHS covers a wide range of activities, including crisis management, information sharing, research and development, and managing the risks posed by our sector's dependency on other critical sectors, such as communications and information technology, for which DHS serves as the SSA. In addition to meeting with senior officials at DHS, the FSSCC and FS-ISAC have engaged in numerous projects and initiatives to improve critical infrastructure and cybersecurity, including:

*Information Sharing and Threat Identification.* On a daily basis, there are cyber attacks. The financial services sector develops its own information about threats, vulnerabilities and incidents. These threats, vulnerabilities and incidences are shared within the protection protocols of the sector. Financial institutions view the risk environment much broader than just within our individual organizations. Given the interconnections and risk exposure among participants and counterparties, an attack on one institution could have cascading implications for others in the sector.

When cyber attacks occur, the FSSCC has a defined crisis management process, escalation and notification protocols to share information. As part of this process, our sister organization, the Financial Services Information Sharing and Analysis Center (known as the "FS-ISAC"), sends rapid notifications to member firms to protect critical systems and assets.

The FS-ISAC reaches more than 20,000 sector participants daily and promotes information sharing between the public and private sectors. The FS-ISAC allows its members to receive threat and vulnerability information immediately; communicate within a secure portal to share vulnerability assessments and other information anonymously; and access new data feeds of threat and vulnerability information. In addition, the FS-ISAC has implemented a crisis communications system to notify its members of emergencies in minutes.

In 2010, the Financial Services Information Sharing and Analysis Center (FS-ISAC), which serves as the information sharing operational arm of the FSSCC, the Department of Defense and DHS, collaborated to launch the Government Information Sharing Framework initiative (GISF) based on initiatives with the Defense Industrial Base (DIB). This pilot program consists of information sharing of threat and attack data between the Federal Government and about a dozen financial services firms. Beyond this, the FS-ISAC is the third sector (following the Communications and IT sectors) to embed at the classified level, senior and operational representatives within the DHS National Cybersecurity and Communications Integration Center (NCCIC) as core members of the watch and response teams. The government's plan is to use these examples as models for public-private sector information-sharing for other sectors to follow.

In early April, senior DHS officials and the FSSCC agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. This decision to collaborate arose in response to a review of lessons learned from recent cyber attacks, which I will review in greater detail later in my testimony. In addition, the FSSCC is working with the National Infrastructure Assurance Council (NIAC) on an information sharing study.

*Sponsoring Security Clearances for Industry Professionals.* At the urging of the FSSCC years ago, DHS and the Treasury have increased the number of clearances for senior executives and experts from our sector. In addition, DHS and the Treasury have arranged classified level briefings each year, typically in conjunction with the FSSCC and FBIIC meetings. Dozens of FSSCC members and all member firms represented on the FS-ISAC Threat Intelligence Committee (TIC) are cleared to at least the SECRET level. In addition, at least seven financial services private sector individuals with cyber security responsibilities are cleared at TOP SECRET/SCI level. For those individuals who have been cleared, the process took a significant amount of time (not to mention the time and expense from the government side).

*Collaborate on R&D.* The FSSCC R&D Committee has been working closely with the Science and Technology Directorate of DHS for many years. Our collaboration began in 2005 when the FSSCC established an R&D Committee and shared the results of our efforts to identify the top R&D priorities.<sup>3</sup> Recently, we have focused considerable attention on improving identity assurance. Our collaboration resulted in a groundbreaking Memorandum of

---

<sup>3</sup> See <https://www.fsscc.org/fsscc/news/default.jsp> for the list of top R&D priorities including: advancing the state of the art in designing and testing secure applications; making financial transaction systems more secure and resilient; improving enrollment and identity credential management; understanding human insider threats and developing deterrence and detection; developing data-centric protection strategies to better classify and protect sensitive information; devising better measures of the value of security investments; and developing practical standards to reduce risk and enhance resiliency.

Understanding (MOU), which was signed on December 6, 2010 by the FSSCC, DHS, and the National Institute of Standards and Technology (NIST) with active support by the White House Cybersecurity Advisor and head of the Office of Science and Technology Policy.<sup>4</sup> The MOU lays the foundation for developing an identity assurance test bed that will focus on improving the accuracy and timeliness of identity proofing, and reducing identity impersonation. The collaborative initiative includes the concept of a “financial services credential verification gateway” to enable direct verification of identity credentials with the authenticating authorities.

As a follow-up to the MOU, the FSSCC is working with DHS and NIST on a Cooperative Research and Development Agreement (CRADA) on identity proofing. Also envisioned in the MOU is an effort to define and test the concept of establishing a secure domain within the larger Internet, where critical industries and government can more securely exchange sensitive information and complete high risk transactions. This effort also includes planning and testing for IPv6 and DNSSEC transitioning.

Other R&D activities include establishing and/or expanding relationships with academia, DHS, National Science Foundation (NSF), NIST, and the Department of Defense’s Networking and Information Technology Research and Development (NITRD) to provide financial services expertise and enhance the transfer of promising research into commercial use. In addition, members of the FSSCC have participated in an insider threat study that DHS’s U.S. Secret Service has been conducting for several years.

*Comments on Strategies and Cyber Incident Response Plans.* The FSSCC has worked with DHS and White House officials in commenting on the National Strategy for Trusted Identities in Cyberspace (NSTIC). The FSSCC also has provided input into the National Cyber Incident Response Plan and supported the National Security Telecommunications Advisory Committee (NSTAC) Cross Sector Information Sharing Pilot.

*Cross Sector Coordination.* The FSSCC continues to work with cross-sector councils. For example, the FSSCC and FS-ISAC participate in the DHS Cross Sector Cyber Security Working Group (CSCWG), which has representation across the 18 critical infrastructure sectors and meets monthly to review cross sector cyber security strategies, programs and projects of interest. From a crisis management perspective, the FS-ISAC presence in both the National Infrastructure Coordination Center (NICC) and the NCCIC supports close cooperation and coordination for disaster, physical security and cyber security events. We also are working with the other critical sectors through the Partnership for Critical Infrastructure Security (PCIS), an “arm” of DHS’s partnership structure outlined in the NIPP, to share critical contact information for each sector as a first step to developing an efficient all hazards cross-sector crisis response plan.

In 2010, a more formal cross-sector information sharing pilot was funded by the President’s National Security Telecommunications Advisory Committee (NSTAC). Four sectors participated in this pilot: financial services, communications, IT, and the defense industrial base. The FS-ISAC provided the secure portal by which the four sectors exchanged cyber threat data. Relevant and actionable cyber threat information was

---

<sup>4</sup> See <http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation>

exchanged during the pilot, which would not have been known to the other sectors. As a result of the program's success, the pilot was extended in 2011 with the intent of rolling it out to all interested sectors later in the year. Furthermore, the FSSCC is involved in cross-sector work of the PCIS in order to share critical contact information for each sector as a first step to developing an efficient cross-sector crisis response plan.

*Participation in Cyber Exercises and Crisis Playbooks.* The financial services sector has performed multiple exercises testing various perceived vulnerabilities and establishing follow-up actions as a result of lessons learned. Significant tests were run to evaluate sector preparedness related to social engineering attacks, payment processing attacks, and communication during a crisis. In particular, the 2009 Cyber Financial Industry and Regulators Exercise (CyberFIRE) and Cyber Attack against Payment Processes (CAPP) exercise were jointly executed by the FSSCC, FS-ISAC, and included many FBIIC members, the U.S. Secret Service, the Federal Bureau of Investigation (FBI), DHS, and more than 800 individual participants. Members of the FSSCC are also planning to participate in the upcoming National Level Exercise #13 in May. The FSSCC and FS-ISAC have created crisis response playbooks in order to clarify lines of communication during crises. The sector provided leadership for recent events requiring a coordinated response, including the earthquake in Haiti, pandemic flu, and hurricane situations.

*Support for Regional Coalitions and Fusion Centers.* Since 2002, the FBIIC and the FSSCC have supported the formation of regionally-based financial partnerships and coalitions dedicated to enhancing the resilience of the financial community in specific geographic areas. At present, there are nearly two dozen regional coalitions that consist of private sector members who partner with the public sector. DHS and the Treasury Department have been very supportive of these organizations, primarily through the Regional Partnership Council (RPC*first*), the umbrella organization to which the coalitions belong. Chicago FIRST, as the Chair of RPC*first*, partnered with the DHS National Cyber Security Division (NCSA) to develop "cyber tabletop in a box." Regional coalitions are conducting these tabletop exercises involving federal, state, and local law enforcement in their respective regions. In addition, there are 72 fusion centers where experts from various federal and local government agencies share information and collaborate with private sector participants.

*Supply Chain Risks.* One of the emerging issues that FSSCC members are evaluating is the security of the global supply chain. Members continue to seek better assurances from our vendors that the major information technology and communications hardware and software systems that we deploy in our networks employ secure development practices and are free from malware or other threats that may have been implanted in the supply chain process. For example, in 2010, the sector published, the *Resilient International Telecommunications Guidelines for the Financial Services Sector*, highlighting the international risks associated with the undersea cables network.<sup>5</sup> This report identified both the risks associated with a critical infrastructure component, provided guidelines for managing those risks, and the need for increased international collaboration. The FSSCC worked closely with FBIIC members, most notably the Federal Reserve Board, and the

---

<sup>5</sup> See <https://www.fsscc.org/fsscc/publications/default.jsp>.

National Communications System, a division of DHS, that works closely with major telecommunications providers.

### **Information Sharing Lessons Learned from Recent Cyber Attacks**

Information sharing is of critical importance to the financial services sector, other critical infrastructure sectors and the government. Without it, none of the FSSCC's other top priorities -- crisis event management, threat matrix dissemination and management, identity assurance -- would be achievable. Although we have made good progress in creating information sharing entities, to share information securely and efficiently, we have not adequately tackled the critically important issues associated with the timeliness and completeness of information. We now need to focus on clarifying and compartmentalizing information so that "actionable intelligence" can be disseminated to responsible parties that will use it to protect critical infrastructure. What I mean by "actionable intelligence" is redacted technical information and contextual information without revealing sources and uses or tipping off criminals or adversaries.

Information sharing among financial institutions, other critical infrastructure sectors, and the government is important for several reasons. First, a company that is a victim of a cyber attack is concerned about protecting its customers, its reputation and complying with regulatory requirements. Second, others in the sector are concerned about the impact that this a cyber attack could have on its organization and counterparties or provider might have on their operations, as well as the potential for systemic risk to entire financial services sector. Third, the government is responsible for enforcing laws and promoting protecting critical infrastructure protection. The government also holds important information that is both technical, such as malware signatures, and contextual, such as what type of entity appears to be initiating the attack. This is due to the governments own operations in cyberspace and other roles including law enforcement, defense and regulation.

There is a strong need to establish appropriate and well-understood protocols to share information so that we collectively understand the problems and risks that we face in order to arrive at the right response or solution. The fundamental issue of striking a balance between confidentiality for criminal investigations and timely information sharing remains a work in progress.

An example of an incident where too much secrecy led to an increased exposure was the cyber attack on a major exchange, which was discovered by the exchange in October 2010. The exchange alerted its primary regulator and law enforcement. For a variety of reasons, including an investigation of the attack by law enforcement and intelligence agencies, information about the attack and its impact on other financial institutions was not disclosed to others in the financial services sector for 102 days. This 102 day period included year-end, when financial institutions closed their books and prepare annual reports. This could have had an enormous impact on employees, stockholders, large and small, and the market as a whole. The lack of meaningful information for more than three months left the entire sector unnecessarily vulnerable.

In response to this event and recent discussions with senior DHS officials, the FSSCC and DHS have agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. FSSCC members believe that a more transparent decision-making process would accelerate the dissemination of information without interfering or undermining criminal and national security investigations. We also hope that these protocols will elevate the priority that government places on sharing information associated with protecting critical infrastructure. Also, by leveraging the security clearances that DHS and other government agencies have sponsored for members of the FSSCC, the government could consult with industry experts to better understand the systemic risk implications of the cyber events.

### **Recommendations for Improving Public-Private Partnership**

FSSCC recommends the following activities to improve the public-private partnership with DHS and other government agencies:

*1. Protecting Critical Infrastructure Through Enhanced Information Sharing.* We have made good progress in creating utilities to share information securely and efficiently. However, we have not adequately tackled the critically important issues associated with the timeliness and completeness of information. We now need to focus on clarifying and compartmentalizing information so that it can be disseminated via the FS-ISAC. This is also important for the government to better understand the significance of information, including the impact on the critical infrastructure sectors. We cannot assume the government will know how to evaluate the risks unless experts from the financial services sector (or other CIP sectors) have a seat at the table. We also recognize that there will be times when the government cannot consult with industry sectors and thus there needs to be clarity as to when and how information will be shared.

As noted earlier in my testimony, FSSCC and DHS have agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. Together, we need to learn from the recent breaches and establish guidelines where we have more predictability in knowing when information will be shared.

Building trust and enhancing understanding is a compelling reason for expanding the number of clearances to senior executives and experts in the financial services sector who are in position to “operationalize” timely and relevant threat and attack intelligence. We also urge DHS to establish clearer protocols for the sponsorship of private sector security clearances that are not directly related to a government contract and for non-US citizens. We recognize that this is a fairly new development and one which does not have clear protocols, either among the sponsoring agencies, or in the private sector. A system that would identify and categorize critical job functions into “need to know” status should effectively expand the community of private sector stakeholders who can get early government notification of significant issues. FSSCC members also suggest better “tearline” documents and the availability of classified information on a geographically, disaggregated basis. Moreover, nationality is a consideration not covered under current “cold war” derived clearance protocols as not all the appropriate individual’s in corporate information security group who have a “need-to-know” homeland cyber security information are U.S. citizens. We propose that the clearance mechanism should expand to consider at minimum

clearing individuals from the UKUSA agreement countries (UK, Canada, Australia and New Zealand) and other countries, as possible, based on government to government background check arrangements.

We need to enhance improve information sharing with the communications, information technology and electricity sectors. Currently the FS-ISAC and FSSCC have little to no operational transparency into other sectors. This may somewhat be addressed by the embedding of personnel in the NCCIC however further policy and engagement is required to provide a Common Operating Picture (COP) across those dependent infrastructures.

*2. Conduct more exercises and training.* In addition to clearances and information sharing, we have found that we build greater trust through exercises and training. By routinely engaging in exercises and training through tabletop exercise, meetings, and awareness campaigns we bring the right public and private sector participants together on a regular basis. Working together, building relationships and establishing trust are essential parts of creating a culture that can share useful and timely information. The embedding of financial sector personnel in the NCCIC and NICC is a positive step in that engagement process.

*3. Invest in R&D.* In addition to supporting the MOU and CRADAs on identity assurance, we also encourage the government to look to emerging research on automated methods of attack detection, communication and prevention. As an example of the possibilities that could be considered, DHS released a whitepaper entitled, *Enabling Distributed Security in Cyberspace*. While this was only a concept paper, it suggests a thoughtful, if ambitious vision for the future where: “A healthy cyber ecosystem would interoperate broadly, collaborate effectively in a distributed environment, respond with agility, and recover rapidly. With a rich web of security partnerships, shared strategies, preapproved and prepositioned digital policies, interoperable information exchanges,....a healthy cyber ecosystem could defend against a full spectrum of known and emerging threats, including attacks against the supply chain, remote network-based attacks, proximate or physical attacks, and insider attacks....”<sup>6</sup>

*4. Coordinate efforts internationally.* Cyber security is not an issue that can be defined by geographic or political borders. The National Cybersecurity and Communications Integration Center is slowly making strides in bringing together industry and government operational capabilities under one roof, breathing the same air, to create a cross-sector common operational picture about our cyber threats and vulnerabilities. The FS-ISAC has a seat in the NCCIC, and both FSSCC and FS-ISAC are participating in the Unified Coordination Group that is developing the NCCIC’s information sharing and incident response process.

The FSSCC recognizes that this is a difficult endeavor – one that involves numerous complexities around national security intelligence, legal authorities, regulatory requirements, privacy protections, and contractual restrictions. We are not where we need to be yet, but we are moving in the right direction – to an envisioned end state where private sector members of the NCCIC are able to communicate threat intelligence in real time to their sector partners and coordinate protective or mitigating action jointly with the government and other sectors.

<sup>6</sup> <http://www.dhs.gov/xlibrary/assets/nppd-healthy-cyber-ecosystem.pdf>

## Comments on Cybersecurity Legislation

The committee had also asked for me to comment on cybersecurity legislation. In general, the FSSCC is supportive of policies in which a “rising tide lifts all boats”. By that I mean the government should offer incentives and, in some cases, require minimum security and resiliency standards for utilities that service critical infrastructure sectors. These utilities include entities like Internet Service Providers and others with whom our sector and other critical infrastructure sector are dependent. For example, we need to ensure that these utilities adopt practices to protect networks, manage incidences, and address our long-standing concerns with Internet congestion during a time of crisis.<sup>7</sup> The development of these standards should be driven by private sector, consensus driven bodies. What has been lacking is a comprehensive cross cutting review of the cyber risk, mitigation, and regulatory dynamics across all of the critical sectors to ensure that any “minimum standards” legislation can allow specific security gaps in each sector to be addressed without imposing one-size-fits-all standards that contradict existing sector regulation.

The FSSCC supports the following provisions:

- Commitment to two-way public-private information-sharing and cross-sector information sharing efforts, leveraging the Information Sharing and Analysis Centers (ISACs), the Sector Specific Agencies (SSAs), US-CERT, safe harbors, clearances, and confidentiality guarantees. Such a commitment is vital to facilitate the sharing of actionable and timely information, particularly during cyber emergencies.
- Focused efforts to address critical interdependencies such as our sector’s reliance on telecommunications, information technology, energy, and transportation sectors.
- Leveraging federal cybersecurity supply chain management and promotion of cybersecurity as a priority in federal procurement.
- Public education and cybersecurity awareness campaigns to promote safe computing practices.
- Enhanced international collaboration and accountability in law enforcement and industry, including increased funding for law enforcement and facilitating the development of global cybersecurity standards.
- Increasing funding for applied research and encouraging collaboration with government research agencies on authentication, access control, identity management, attribution, social engineering, data-centric solutions and other cybersecurity issues. It is only through such public-private efforts, combined with adequate funding, that leading edge research in these important areas can enhance our ability to secure online transactions, maintain data integrity, and enhance user confidence.
- Attention to ICANN and other international Internet governance bodies especially as ICANN begins a new application round for what could be as many as a thousand new top-level Internet domains later this year. It is vitally important that effective oversight exist to enhance security and privacy protections.

<sup>7</sup> U.S. Department of Homeland Security, *Pandemic Influenza Impact on Communications Networks Study*, December 2007. <http://www.ncs.gov/library/pubs/Pandemic%20Comms%20Impact%20Study%20-%20Best%20Practices.pdf>; GAO, *Influenza Pandemic: Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet Congestion and Encourage Readiness*, GAO-10-8, October 2009. <http://www.gao.gov/new.items/d108.pdf>.

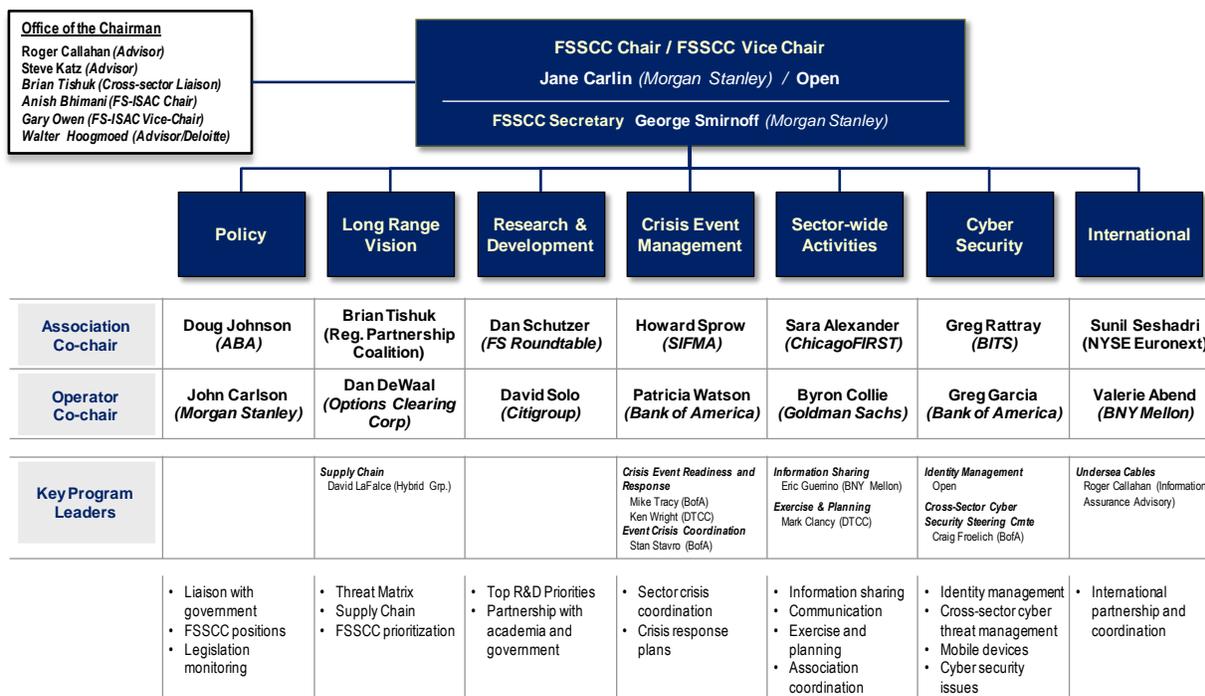
- Need for enhanced supervision of service providers on whom financial institutions depend, while at the same time recognizing the role of federal financial regulators in issuing regulations and supervisory guidance on security, privacy protection, business continuity, and vendor management for financial institutions and for many of the largest service providers. Strengthening government-issued credentials (e.g., birth certificates, driver's licenses and passports) that serve as foundation documents for private sector identity management systems.

The FSSCC does not support provisions that provide sweeping new authority for the Executive Branch to remove access to the Internet and other telecommunications networks, without clarifying how, when and to what extent this would be applied to our critical infrastructures. Such a provision also sets the wrong precedent in light of recent restrictions on Internet use imposed in other countries.

## **Conclusion**

In conclusion, I would like to thank the committee for inviting me to testify today on behalf of the FSSCC on the DHS cybersecurity mission and how they interact with private sector owners. Both the public and private sector financial services organizations recognize the importance of improving information sharing as part of continuity planning, crisis management, and enhancing resiliency in preparing for and responding to significant events. We know that during a real crisis we cannot operate as independent entities and thus we must establish trusted relationships and plan ahead of time so that we are prepared to respond to a real crisis. It is my hope that the good work done to date in bridging the public-private divide by FSSCC and DHS continues and that we find additional ways to effectively combat those who would seek to undermine our economy and stability—be they homegrown or foreign, criminal or terrorist, rogue or state-sponsored. It is only by working together that we will prevail in the complex and every changing internet-connected world.

## Appendix A: FSSCC Org Chart



## Appendix B: Executive Summary of Sector Annual Report

### Executive Summary

In 2003, the Banking and Finance Sector, hereinafter referred to as the Financial Services Sector, was identified as a critical infrastructure sector pursuant to Homeland Security Presidential Directive 7 (HSPD-7); the U.S. Department of the Treasury was identified as the Sector-Specific Agency (SSA) for the sector. As the SSA, the Treasury Department works with its public and private sector partners to maintain a robust sector that is resilient against manmade or natural incidents. The Financial Services Sector is essential to the efficiency of world economic activity. This Sector Annual Report outlines the requirements for current and future protective programs based on HSPD-7.

Both the private and public sectors, through the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the Financial and Banking Information Infrastructure Committee (FBIIC), respectively, have key roles in implementing the Financial Services Sector's critical infrastructure and key resources (CIKR) protective programs. Through direct mandates and regulatory authority, Federal and State financial regulators have specific regulatory tools that they can implement in response to a crisis. In addition, the Department of the Treasury – along with the FBIIC, the FSSCC, Financial Services Information Sharing and Analysis Center (FS-ISAC), and regional partnerships – have developed and continue to implement numerous protective programs to meet the Financial Services Sector's goals. The protective programs range from developing and testing robust emergency communication protocols, to identifying critical Financial Services Sector threats, to addressing cybersecurity protection needs. The success of the public-private partnership has proven critical to the Financial Services Sector's achievements through one of the most challenging periods for the sector with respect to credit and liquidity risks.

The scope of the Financial Services Sector includes public and private institutions involved in carrying out the primary sector functions of clearing, payment, settlement, and trading. Multiple organizations perform these functions and collectively represent the Financial Services Sector.

- Clearinghouses
- Commercial banks
- Credit rating agencies
- Exchanges/electronic communication networks
- Financial advisory services
- Insurance companies
- Financial utilities
- Government and industry regulators
- Government subsidized entities
- Investment banks
- Merchants
- Retail banks
- Electronic payment firms

Through the public-private partnership, the following vision statement for the Financial Services Sector has been established.

### Vision Statement

*To continue to improve the resilience and availability of financial services, the Banking and Finance Sector will work through its public-private partnership to address the evolving nature of threats and the risks posed by the sector's dependence on other critical sectors.*

The Financial Services Sector pursues this vision by working toward its three sector goals:

1. To achieve the best possible position in the face of myriad intentional, unintentional, manmade, and natural threats against the sector's physical and cyber infrastructure;
2. To address and manage the risks posed by the dependence of the sector on the Communications, Information Technology, Energy, and Transportation Systems Sectors; and
3. To work with the law enforcement community, financial regulatory authorities, the private sector, and our international counterparts to address threats facing the Financial Services Sector.

In support of the sector goals, the FSSCC has recently updated its mission and objectives, as is further described in Section 3. Representing the strategic arm of the Financial Services Sector, the FSSCC has established the following objectives:

- Identify Threats and Promote Protection
- Drive Preparedness
- Collaborate with the Federal Government
- Coordinate Crisis Response

The Financial Services Sector's goals and objectives guide our activities in managing significant sector risks. Significant sector risk considerations have been identified and are described in greater detail in Section 2. They are summarized as follows:

- |                      |                             |
|----------------------|-----------------------------|
| ▪ Confidence Risk    | ▪ Infrastructure Risk       |
| ▪ Concentration Risk | ▪ Geographic Proximity Risk |
| ▪ Supply Chain Risk  | ▪ Technology Risk           |

Management of these risks has resulted in the identification of the following potentially significant sector vulnerabilities:

1. Confidentiality – Maintaining the confidentiality of clients and meeting all legal requirements for maintaining confidentiality;
2. Integrity – Ensuring transactional integrity to support financial transactions; and
3. Availability – Ensuring that financial services are available to maintain the smooth flow of capital.

The sector's goals, initiatives, and activities are in pursuit of achieving the four objectives identified above to effectively manage sector risks and vulnerabilities.

The following sections summarize the significant activities that are described in subsequent chapters of this Financial Services Sector Annual Report.

## ES.1 Strategic Goals

Over the past year, the Financial Services Sector set forth the following objectives and goals that drive the FSSCC activities and guide activities of the sector's multiple organizations.

Strategic Objectives	2010 Goals
<b>Identify Threats and Promote Protection</b>	<ul style="list-style-type: none"> <li>▪ Finalize updated Threat Matrix</li> <li>▪ Disseminate Threat Matrix and build into strategy</li> <li>▪ Build Threat Matrix into ongoing planning and execution of FSSCC goals</li> </ul>
<b>Drive Preparedness</b>	<ul style="list-style-type: none"> <li>▪ Establish regularized process for escalating events and disseminating information in the form of actionable intelligence</li> <li>▪ Establish more direct international relationships</li> <li>▪ Further the undersea cables work</li> <li>▪ Develop supply chain frameworks</li> <li>▪ Disseminate CyberFIRE and Cyber Attack against Payment Processes (CAPP) Exercise learning</li> <li>▪ Support regional coalitions</li> </ul>
<b>Collaborate with the Federal Government</b>	<ul style="list-style-type: none"> <li>▪ Establish ongoing interaction with (1) the new White House Cybersecurity Coordinator and (2) DHS/National Security Agency (NSA)</li> <li>▪ Address Internet congestion as part of DHS interaction</li> <li>▪ Develop Identity Management Principles and request for investment</li> <li>▪ Implement Government Information Sharing Framework initiative with Department of Defense (DoD) and DHS</li> <li>▪ Develop sector-wide position on Internet Corporation for Assigned Names and Numbers (ICANN)</li> <li>▪ Engage in conversation on cyber and critical infrastructure legislation and determine appropriate next steps</li> <li>▪ Deliver a finance and banking educational session</li> </ul>
<b>Coordinate Crisis Response</b>	<ul style="list-style-type: none"> <li>▪ Expand and improve crisis management response playbooks</li> <li>▪ Improve usefulness and mindshare of playbooks</li> </ul>

### **ES.1.1 Identify Threats and Promote Protection**

The Financial Services Sector is developing a comprehensive All-Hazards Threat Matrix accounting for over 1,900 individual threats. A risk ranking methodology is being used that can be applied at the sector level and adopted by individual organizations to adapt to their specific needs. As a major initiative for the sector, begun in 2009, it will continue throughout 2010 and serve as the foundation for strategic efforts going forward.

Additionally, the sector published the *Resilient International Telecommunications Guidelines for the Financial Services Sector* (Undersea Cables Report), highlighting the international risks associated with our undersea cables network. This significant report highlights both the risks associated with a critical infrastructure component and the need for increased international collaboration.

Additionally, the sector has elevated its focus on cybersecurity. Several exercises have been run to identify cyber threats, and research and development (R&D) efforts have been focused on addressing vulnerabilities through a collaborative public-private joint effort. The sector made significant contributions to the National Cyber Incident Response Plan, created new FSSCC working groups focusing on Identity Management and Supply Chain issues, and engaged with the Director of National Intelligence and the Intelligence Community on multiple cyber issues.

### **ES.1.2 Drive Preparedness**

The sector has performed multiple exercises testing various perceived vulnerabilities and establishing follow-up actions as a result of the learning. Significant tests were run to evaluate sector preparedness related to social engineering attacks, payment processing attacks, and communication during a crisis. In particular, the Cyber Financial Industry and Regulators Exercise (CyberFIRE) and Cyber Attack against Payment Processes (CAPP) Exercise were jointly executed by the FSSCC, FS-ISAC, and FBIIC and included the U.S. Secret Service, the Federal Bureau of Investigation (FBI), and the U.S. Department of Homeland Security (DHS), plus more than 800 individual participants.

Sector crisis response playbooks have been created and strategic and tactical efforts have been delivered to clarify lines of communication critical in crisis response. The sector coordinated over 45 operators and associations and performed multiple other FS-ISAC and regional exercises throughout the year.

### **ES.1.3 Collaborate with the Federal Government**

The Financial Services Sector has stepped up its partnership with the U.S. Government, academia, and related sectors. The sector has established successful working relationships with academia, the National Institute of Standards and Technology (NIST), the Department of Homeland Security, the National Science Foundation (NSF), and the Networking and Information Technology Research and Development (NITRD) program; participated in a

roundtable with the DHS Secretary; and established a working dialogue with the White House's Office of Science and Technology Policy (OSTP) through Aneesh Chopra.

The sector has further contributed significantly to government-led initiatives in identity management and the development of incident response plans. Coordination among intelligence agencies, regulators, other government agencies, and the private sector has received considerable focus and is a hallmark of the sector's achievements.

The FS-ISAC has collaborated with DoD and DHS to launch the Government Information Sharing Framework initiative. This pilot program has been implemented in 2010 and consists of large-scale information sharing of threat and attack data between the Federal government and financial services firms that have agreed to participate. The government's plan is to use this as a public-private sector information-sharing model for other sectors and other Federal government agencies to follow.

#### **ES.1.4 Coordinate Crisis Response**

The sector collaborated to develop crisis response plans for all hazards, as well as specific plans for hurricanes. The sector provided leadership for recent events requiring a coordinated response, including Haiti, pandemic flu, and hurricane situations.

#### **ES.1.5 Conduct Research and Development**

Led by the FSSCC R&D Committee, the sector has identified and progressed on seven R&D priorities it has established (further described in Section 5):

- Advancing the State of the Art in Designing and Testing Secure Applications
- Making Financial Transaction Systems More Secure and Resilient
- Improving Enrollment and Identity Credential Management
- Understanding Human Insider Threats and Developing Deterrence and Detection
- Developing Data-Centric Protection Strategies to Better Classify and Protect Sensitive Information
- Devising Better Measures of the Value of Security Investments
- Developing Practical Standards to Reduce Risk and Enhance Resiliency.

The FSSCC R&D Committee has proposed to senior White House and other Government officials a public-private sector collaboration to improve identification validation and has drafted a proposal on an identity credential verification gateway. Further, it participated in the Federal government's National Cyber Leap Year Summit and put forth the Financial Communications and Authentication Pilot ("testbed") in response to discussions among the FSSCC R&D Committee, senior White House personnel, and NIST and DHS officials.

Outreach for R&D efforts has been significantly expanded. Several comment letters have been sent, and engagements have occurred with multiple government organizations, including the U.S. Department of State on "Current Challenges and Future Strategies for Improving Identity Management," the Critical Infrastructure Protection Congress on

identity management, and the Internet Corporation for Assigned Names and Numbers (ICANN) on the expansion of top-level domains, among others.

## **ES.2 Sector Challenges and Looking Forward**

Looking forward to the next year, the Financial Services Sector will build on its substantial success achieved in the past year. While priorities will be set later in the year, significant efforts are expected to focus on the following:

- Evaluating the top threats to the Financial Services Sector
- Coordinating multiple government activities
- Researching internet congestion
- Investigating ICANN proposals to expand top-level domains
- Exploring identity management issues
- Expanding international coordination