CQ Congressional Testimony

October 31, 2007 Wednesday

CYBERSECURITY ISSUES

SECTION: CAPITOL HILL HEARING TESTIMONY

LENGTH: 4577 words

Statement of George Hender Management Vice Chairman Options Clearing Corporation

Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

October 31, 2007

Chairman Langevin, Chairwoman Jackson-Lee, Ranking Members McCaul and Lungren, and members of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology and the Subcommittee on Transportation Security and Infrastructure Protection of the House Homeland Security Committee, I am George Hender, Management Vice Chairman of The Options Clearing Corporation (OCC), which is the world's largest derivatives clearing organization. OCC is a leader in business continuity planning in the financial services sector and was a founding member of the Financial Services Sector Coordinating Council (FSSCC) and ChicagoFIRST, a regional public/private partnership addressing homeland security and emergency management issues in the financial services industry. I am pleased to submit this statement on the very important topic of cybersecurity on behalf of FSSCC.

On June 6, 2006, I was appointed to serve as Sector Coordinator for the Financial Services Sector by former Secretary of the Treasury John Snow. Thus, I am the Chairman of FSSCC. Prior to my appointment, I served as FSSCC's Vice Chairman from September 2004 through May 2006. Additionally, I am 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 infrastructures. I have also formerly served as Vice Chairman of the Financial Services Information Sharing and Analysis Center (FS-**ISAC)**. This is the organization responsible for communicating key cyberspace, physical security, and Homeland Security information to the financial services sector.

I applaud the Committee for holding today's hearing on such an important topic. Before I focus on measures taken by FSSCC related to cybersecurity, I would first like to discuss the important role the financial services sector has in our economy and the role FSSCC plays in improving the sector's resilience through safeguarding its critical infrastructure and employees.

Introduction and Background

The United States financial services sector is the backbone of the world economy.

With United States assets estimated to be in excess of $55 trillion, this

large and diverse sector accounted for over $1 trillion in 2006 gross domestic product (GDP) or 7.8 percent of total GDP. The sector is primarily owned and operated by the private sector whose institutions are extensively regulated by Federal and, in many cases, state government. 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), and the National Futures Association (NFA), and exchanges, such as the Chicago Mercantile Exchange (CME), the New York Stock Exchange (NYSE), also play an important role in industry oversight.

Working together, the public and private sector regulators encourage a highly competitive market where identifying and managing a myriad of financial and nonfinancial risks is essential to success. Through numerous laws enacted by Congress over the past 150 years, federal financial regulators have implemented a complex regime that includes examinations of the sector's institutions' operational, financial and technological systems. These examinations are designed to determine the extent to which an institution is addressing its financial and non- financial risks, such as Internet and information technology vulnerabilities. They also evaluate the adequacy of controls and applicable risk management practices at the institution.

Public-Private Partnership

Both the public and private sector financial services organizations recognize the importance of business continuity planning in preparing for catastrophic events; however, our sector's organizations know they will not operate as independent entities during a real crisis. Therefore, planning for these events should be done in a coordinated fashion.

FSSCC was established at the request of the U.S. Treasury Department in response to Homeland Security Presidential Directive 7, which required sector-specific Federal departments and agencies to identify, prioritize and protect United States critical infrastructure and key resources. We are a private sector coalition of the nation's leading financial services firms and trade associations that are working to reinforce the financial services sector's resilience to terrorist attacks, man- made and natural disasters, and other threats, such as cyber attacks, facing the sector's critical infrastructure.

FSSCC closely interacts with its Sector Specific Agency (SSA), the Department of the Treasury (Treasury), and the Financial and Banking Information Infrastructure Committee (FBIIC), its public- sector counterpart. We also strongly support regional public/private partnerships, such as ChicagoFIRST and DFWfirst. These organizations address homeland security and emergency management issues on a local level, where many catastrophic events are primarily managed.

The combined efforts and close interaction of these groups with FSSCC fosters a spirit of cooperation within our sector that facilitates effective preparation for a critical event, such as a cyber attack. Equally important, this collaboration creates a streamlined approach to working with other sectors where cross- industry interdependencies exist.

The financial services sector is very dependant on a number of other sectors, especially the energy, telecommunications and transportation sectors.

At the beginning of my term as FSSCC Chairman, I personally met with representatives from nearly every FSSCC member to solicit their ideas on how to further strengthen the resilience of the financial services sector and reduce vulnerability to cyber threats, terrorist attacks, criminal or illegal activities, and man-made or natural disasters.

These conversations, as well as the large number of formal and informal meetings taking place each year within FSSCC and between FSSCC and FBIIC, help show how our partnership model addresses threats and risks posed by the Sector's dependency upon other sectors.

FSSCC's general meetings provide an example of this model. Here members meet and hear from critical sectors on which our sector heavily relies. They also provide a venue in which to coordinate and prioritize sector initiatives. Another example is the FSSCC working group which is working with the Department of Homeland Security (DHS) to develop an emergency credential for FSSCC members' use in extraordinary emergencies. Development of such a credential is a priority reflected in our overall research plan. Just this last summer, the FSSCC credentialing working group participated in the cross-sector exercise known as "Summer Breeze." This exercise validated the use of First Responder Authentication Credential (FRAC) identification cards.

Arguably, the most important example of collaboration within the sector is the ongoing effort to plan for pandemic influenza. On October 12, 2007, FSSCC and FBIIC completed the most comprehensive exercise ever held for the U.S. financial services sector. This important exercise focused on the response of the sector's members to pandemic influenza; over 2,700 financial firms participated. FSSCC understands that effective business continuity planning must envision and prepare for a diverse range of issues and threats. This is encompassed in our mission statement and goals.

FSSCC's Mission and Goals

FSSCC's mission is to foster and facilitate the coordination of sector-wide voluntary activities and initiatives designed to bolster critical infrastructure protection and homeland security. FSSCC strives to improve sector awareness of critical infrastructure protection issues, to promote information sharing on these issues, and to find opportunities for improved coordination throughout the sector. Through its efforts, FSSCC seeks to enhance public trust and confidence in the sector's ability to withstand and recover from significant disasters.

Treasury, in close collaboration with FSSCC and FBIIC, completed the Banking and Finance Sector's Sector Specific Plan (SSP) in December 2006. This plan, combined with the 16 other critical infrastructure SSPs, helps form the overall National Infrastructure Protection Plan (NIPP). Our sector's SSP outlines a strategy for working collaboratively with public and private sector partners to identify, prioritize and coordinate the protection of critical infrastructure. FSSCC believes DHS appropriately guides each critical infrastructure sector in coordinating their SSPs. However, each sector specific agency should retain control over SSP implementation. Also, DHS and each sector should view the SSPs as a starting point for developing a comprehensive, nationally-oriented, critical infrastructure regime.

The Banking and Finance Sector's SSP, including its Research and Development (R&D) appendices, outlines three sector-specific goals. First, the sector seeks to maintain its strong position of resilience, risk management and redundant systems, in the face of a myriad of intentional, unintentional, man-made and natural threats. Second, the sector aims to address and manage the risks posed by the sector's dependency on telecommunications, information technology, energy and transportation sectors. Lastly, the sector plans to continue to work with the law enforcement community, the private sector, and our international counterparts to increase available resources used to track and arrest criminals. Specifically, to track and arrest those persons responsible for crimes against the sector, including cyber attacks and other electronic crimes.

The remainder of my testimony will focus on FSSCC's efforts in addressing these goals in light of protecting against cyber attacks and other electronic crimes.

Specific Actions for Cybersecurity

Modern financial services are built on a foundation of information technology, including computing hardware, software and telecommunications. This foundation is afflicted by multiple vulnerabilities and an increasingly high level of threats. Our sector's cybersecurity strategy seeks to address these threats by generally focusing on people, process and technology. Ensuring our sector has the brightest minds, most efficient processes and state-of-the-art technology to protect against cyber threats is our highest priority because our sector understands our entities' systems and networks are a target because "that's where the money is." In addition, as September 11, 2001, showed us, our sector is a focus of terrorists because of our iconic status.

Our sector faces a number of cyber-related threats such as, hacking, virus dissemination, software piracy, identity theft, account fraud, phishing, spoofing, and pump and dump schemes. FSSCC's members have responded to these challenges aggressively. For example, FSSCC member organizations have prepared a document to help financial institutions develop and execute response programs when confidential and sensitive information is accessed or misused by unauthorized individuals. The Identity Theft Assistance Center, developed by a FSSCC member, provides a free victim assistance service and provides data about identity theft to law enforcement.

The financial services sector has always placed itself on the cutting edge of cybersecurity initiatives. Our institutions were among the first to have Chief Information Security Officers as part of their management teams. Also, the sector was among the first to use various authentication tools to protect against internet fraud. Similarly, many financial institutions embrace the concept of layered security by using multiple intrusion detection and prevention products. Firms regularly work with technology companies to improve these products. Without such security measures in place, customers would hesitate to use on- line products which are a central component of a financial firm's business model. In addition to the threat to individual customers, our sector is also focused on cyber-related threats to our financial structure. The nature and complexity of attacks are growing more sophisticated. As a result, our sector works in close collaboration with the nation's intelligence community to address this concern.

FSSCC R&D Committee

Prior to the NIPP's issuance in June 2006, FSSCC recognized cybersecurity as a critical issue and formed a standing R&D Committee. This committee was established to identify and prioritize areas of need, in which the most promising opportunities exist for research and development initiatives. These initiatives significantly improve the sector's critical infrastructure protection. The R&D Committee began developing a list of priorities in 2005. In April 2006, the committee published Research Challenges, a document which identifies eight R&D areas the sector needs to address.

An over-arching theme throughout our Research Challenges is securing the sector's information technology infrastructure to prevent intrusion from unauthorized sources. In October 2006, the FSSCC R&D committee, with Treasury advising, demonstrated for DHS how FSSCC's Research Challenges related to the NIPP by publishing FSSCC's Research Agenda. Together these two publications provide industry, academia, and the public with a shared insight into the

opportunities and requirements necessary to produce a robust cybersecurity platform.

FS-ISAC

The FS-ISAC is another vital asset to FSSCC and the sector. It was created on October 1, 1999, as a means of meeting the sector's information-sharing obligation under the 1998 Presidential Decision Directive 63 on Critical Infrastructure Protection.

The FS-ISAC channels information from more than 100 sources to reach over 11,000 sector participants daily and promotes information sharing between the public and private sectors. The FS-ISAC provides sector-wide knowledge about cyber and physical security risks faced by the financial services sector. Specifically, FS-ISAC's incident alerts notify members about the type of attack, its origin, and suggested remedial action.

FS-ISAC information allows members to immediately receive threat and vulnerability information; share vulnerabilities anonymously and communicate within a secure portal; access new data feeds of threat and vulnerability information; and access a wide range of user data from which users can produce their own reports and metrics. The FS-ISAC also uses this information to work with Treasury and law enforcement in helping to stop and prevent attacks.

Two important government information sources for the FS-ISAC's 24/7 Security Operations Center are DHS's Homeland Security Information Network (HSIN) and the U.S.-Computer Emergency Readiness Team (US-CERT). Relevant information from these data sources is monitored by the FS-ISAC and shared with trusted sector representatives through FS-ISAC's notification system and web portal. Then reports from FS-ISAC approved members are uploaded through the system. Both sources provide a valuable service to the FS-ISAC. FSSCC and the FS-ISAC continue to work with DHS to coordinate these reports into the sector's information sharing structure.

The FS-ISAC has been an effective tool in the fight against cyber attacks. For example, in November 2006, an FS-ISAC member detected an unusually large number of unauthorized log-in attempts against its systems and anonymously reported this information to the FS-ISAC. Soon after, the FS-ISAC issued an alert to its members.

Later, five more financial institutions reported similar activity. This information sharing proved the financial institutions were under attack from a single source. While the attack was relatively insignificant in terms of its potential sector-wide impact, it demonstrates how the FS-ISAC's collaborative model can be an effective means to quickly deliver real-time information so financial institutions may be alerted to act against real threats.

The FS-ISAC was effective once again this past August when it alerted several member banks of suspicious web-site activity. The FS-ISAC then helped to avoid compromise of several major money center and regional banking institutions user accounts.

Cyber Syllabus

In May 2006, the U.S. Department of Defense sought a private sector partner to help develop an undergraduate studies curriculum designed to provide exposure to information technology cybersecurity issues. FSSCC, through its R&D Committee, took the initiative to partner with the National Terrorism Preparedness Institute at St. Petersburg College in Florida to complete the project. I am pleased to report the syllabus was completed in May 2007, resulting in an on-line training program that can be made available to all

universities. Additionally, FSSCC is working to identify an educational institution capable of making this program available to our members at no cost. It is our hope this type of public-private collaboration will help to inspire a new generation of ideas and resources devoted to protecting our nation's cyber space.

Handbook of Science and Technology for Homeland Security

Another joint DHS/FSSCC initiative currently underway is the drafting of a handbook designed to educate researchers on the critical needs of the homeland security and intelligence communities. It will also promote interdisciplinary dialogue in those fields. I am pleased to report FSSCC is on target to provide this information to DHS by year's end. Also, this handbook should be distributed worldwide in online and print formats next year.

Cybersecurity Exercises

FSSCC and FS-**ISAC** have been active participants in several business continuity exercises, including the congressionally mandated TOPOFF exercises and a number of regional and national cybersecurity exercises. In February 2006, FS-**ISAC** represented our sector in Cyber Storm, the first government-led, full scale cybersecurity exercise of its kind. Ten months later, in December 2006, FS-**ISAC** participated in Cyber Tempest, an exercise devoted to testing a wide area of cyber issues from a regional perspective.

Both of these exercises provided positive benefits to our sector's business continuity planning, such as developing better integration between FSSCC and the FS-**ISAC.** FSISAC is now involved in planning Cyber Storm II scheduled for March 2008. These opportunities are a vital resource to leverage. We believe exercise leaders would benefit by increasing our level of involvement in future exercises.

PCIS Working Group

FSSCC has been an active participant in PCIS, which was formally recognized in the NIPP as the Private Sector Cross-Sector Council. PCIS is dedicated to coordinating cross-sector initiatives aimed at promoting public and private efforts to improve the security and safety of our nation's critical infrastructure. PCIS has established a working group focused on cross-sector collaboration of cybersecurity issues. Each Sector Coordinating Council must appoint a sector representative to participate on the working group. The FSSCC has selected FS-**ISAC** Chairman, Eric Guerrino, for this task. The PCIS working group is another example of how the financial services sector is following a collaborative model to develop a strong cybersecurity network.

Future Challenges

FSSCC has achieved a great deal over the past few years. However, there are still many issues which must be addressed regarding cybersecurity. Some of these issues have been highlighted in a recent Government Accountability Office (GAO) report entitled Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cybersecurity Elements Varies. Another less apparent, but equally important, issue includes increasing the level of consultation between DHS and its SSCs and SSAs over research and development initiatives. I will take a few moments to highlight each issue.

GAO Report

The GAO recently conducted a review of each SSP to determine if key aspects of cybersecurity related to the NIPP had been adequately covered. The GAO's preliminary results have found none of the plans fully addressed all 30

cybersecurity related criteria. Consequently, the GAO recommends that DHS require all SSPs be amended to address all cyber-related criteria by September 2008. Based on the cyber-related criteria established by GAO for its report, the GAO concluded the Banking and Finance Sector's SSP "somewhat comprehensively" covers cybersecurity. We respectfully disagree with the GAO's analysis. Because the GAO did not consult the SSAs or Sector Specific Councils when conducting its review, I would like to take this opportunity to explain our view on several areas the report concluded our SSP did not address.

Under section seven of the report, GAO stated our sector's SSP failed to 1) describe a process to solicit information on ongoing cyber R&D initiatives and 2) identifies existing cyber-related projects that support goals and identifies gaps. The sector's SSP highlights the R&D committee as the primary mechanism to solicit information on R&D initiatives, and the R&D Committee's Research Challenges outlines in detail the sector's goals and gaps related to cybersecurity. Further, our sector's priority on R&D is evidenced by the establishment of the FSSCC R&D Committee in 2005 and publication of its Research Challenges in April 2006, well before the NIPP was issued last year. FSSCC believes the SSP and the Research Challenges document, which was incorporated into the SSP in an appendix, adequately addresses the GAO's criteria. We welcome a dialogue with the GAO on this issue.

Additionally, GAO's review stated, under section five, that our sector failed to identify programs to deter, respond, and recover from cyber attack. The Banking and Finance Sector SSP used a deter, respond and recover approach throughout all sections.

Our testimony today highlights a number of initiatives mentioned in our SSP aimed at this very issue - the R&D Committee, FS-**ISAC,** Cyber Syllabus, Cyber Threat Exercises, and PCIS. Consequently, without further guidance from GAO it is unclear how they reached a conclusion that our sector completely failed to address this issue.

The GAO report, under section eight, also stated our SSP failed to describe a process for investment priorities. Although FSSCC does not have any budget authority, we believe our R&D Committee's Research Challenges and Research Agenda highlight a number of priorities where investment dollars are most needed for our sector.

FSSCC, FBIIC and Treasury worked in close collaboration to develop our SSP, which we believe memorializes past and current initiatives into a living document serving as a guide for future action. In other words, we agree with DHS's assessment that the SSPs "represent only the early efforts by the sectors to develop their respective plans."

Consequently, we welcome all comments and dialogue from interested parties on how to improve our nation's critical infrastructure protection regime and believe that our sector is a model for less regulated sectors with less mature cybersecurity plans.

SSC/SSA R&D Budget

FSSCC believes DHS should consult with the SSCs, and, at the very least, their SSAs, on business continuity research projects to ensure optimal resource allocation is taking place. FSSCC would like to encourage the Subcommittees and Congress as a whole to work with DHS to ensure the same collaborative model used in our sector to generate business continuity information and reports extends to actual resource allocation for critical infrastructure programs. Failure to consult with experts from the organizations representing each sector severely limits the ability to maximize returns from investment dollars in an efficient

manner.

Over the past few years, FSSCC and its members have devoted significant resources to generating information, developing plans, and identifying issues related to cybersecurity and opportunities for research for the public sector. While much information has been collected, FSSCC fears this information risks being lost in a "black hole." To avoid this result, FSSCC seeks to work with its public and private partners to develop a formal program that would channel resources to areas and programs that would provide the most positive impact for our nation's critical infrastructure. FSSCC thinks that it makes good economic sense to channel available sector and public research resources to programs supporting the Research Challenges and Research Agenda developed by industry experts on FSSCC's R&D Committee. To achieve this goal, greater communication and consultation about opportunities for R&D spending is necessary between DHS, Treasury and FSSCC. Another option would be to provide grant authority to SSAs such as the Treasury Department.

Currently, FSSCC is limited to influencing R&D project funding through support letters. Recently, FSSCC R&D Committee members visited Carnegie Mellon University (CMU) with a Treasury official to introduce CMU officials to the FSSCC R&D Agenda.

While at CMU, the FSSCC R&D Committee reviewed CMU research projects that CMU judged to be of interest to the financial community. Committee members found that CMU projects focused on Operational Resiliency, Keystroke Pattern Analysis, Device- Enabled Authentication, and Insider Threat Analysis specifically addressed major FSSCC research challenges, as well as the corresponding NIPP research agenda themes. FSSCC could not fund these research projects but wrote letters of support to encourage funding from other sources.

FSSCC believes the DHS cybersecurity R&D budget should be more closely aligned with the threat posed. Twelve million dollars appropriated for this purpose is insufficient to cover the R&D demands within DHS and throughout the critical infrastructure sectors. Our nation would be better served by providing additional budget discretion and dollars to those most closely aligned with the work to be performed.

Conclusion

The financial services sector has a long history of thoughtfully and carefully preparing for threats to its critical infrastructure and employees. The members of FSSCC are proud of our progress since our inception in staying abreast of new and unexpected threats to the critical infrastructure of the financial services sector.

The financial services sector is working diligently to refine best practices, business continuity plans, and homeland security efforts to better protect employees and financial assets from cyber attacks. We are grateful for the collaboration and coordination with our public sector partners, the Department of the Treasury and the other members of FBIIC, as we develop these plans. We will continue to work diligently, and I am confident that the financial sector's preparation for cyber attacks will meet the high standards of planning for which our industry is well respected.

Thank you again for the opportunity to provide FSSCC's views for this important hearing. I would be pleased to answer any questions.

LOAD-DATE: November 5, 2007

LANGUAGE: ENGLISH

COMMITTEE: HOUSE HOMELAND SECURITY

SUBCOMMITTEE: EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

TESTIMONY-BY: GEORGE HENDER, MANAGEMENT VICE CHAIRMAN

AFFILIATION: OPTIONS CLEARING CORPORATION