Financial Services Sector Coordinating Council

for Critical Infrastructure Protection and Homeland Security

Oral Statement of

George S. Hender
Chairman

On behalf of the

Financial Services Sector Coordinating Council
(FSSCC)

Before the

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

&

Subcommittee on Transportation Security and Infrastructure Protection

Of the

Committee on Homeland Security

United States House of Representatives

On

"Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans"

October 31, 2007

Oral Statement of George S. Hender, Chairman, FSSCC
October 31, 2007

Chairman Langevin, Chairwoman Jackson-Lee, Ranking Members McCaul and Lungren, and members of both Subcommittees, my name is George Hender, and I'm Chairman of the Financial Services Sector Coordinating Council, also known as FSSCC. I'm pleased to appear today on FSSCC's behalf to discuss the important topic of cybersecurity.

FSSCC was established at the request of the Department of Treasury and its mission is to coordinate sector-wide voluntary activities related to critical infrastructure protection. FSSCC is a private-sector coalition of the nation's leading banks, financial firms, insurance companies and their trade associations.

FSSCC worked collaboratively with Treasury, our sector specific agency, and with FBIIC, our government coordinating council, to craft our Sector Specific Plan. Our plan identifies three sector-specific goals: to maintain our sector's strong position of resilience, risk management and redundant systems; to manage the risks posed by cross-sector interdependencies; and, to work with law enforcement, the private sector, and our international counterparts to track and arrest criminals.

The remainder of my testimony will focus on FSSCC's efforts to meet these goals in the area of cybersecurity.

Specific Actions for Cybersecurity

Modern financial services are built on a foundation of information technology. Financial firms systems are a target for cyber attacks because "that's where the money is." As the nature and complexity of attacks grow more sophisticated, FSSCC continues to implement a number of cyber-related initiatives. I'd like to highlight some of our initiatives.

<u>FSSCC R&D Committee</u>

A year prior to the National Infrastructure Protection Plan's release in 2006, FSSCC formed a standing R&D Committee. In April 2006, the committee published *Research Challenges,* a report identifying eight sector-specific R&D priorities.

An over-arching theme throughout this report is protecting the sector from cyber attacks. In October 2006, the R&D Committee published FSSCC's *Research Agenda* to demonstrate how *Research Challenges* related to the NIPP. Together these two publications provide interested stakeholders with the necessary steps to produce a robust cybersecurity platform.

FS-ISAC

Another vital asset to FSSCC and the sector is the Financial Services Information Sharing and Analysis Center. Our ISAC has been an effective information sharing tool in the fight against cyber attacks. Every day our ISAC forwards cyber and physical security risk updates from more than 100 sources to over 11,000 sector participants. Our ISAC also shares this information with Treasury and law enforcement to help stop and prevent attacks.

Cybersecurity Exercises

FSSCC and our ISAC have also been active participants in several business continuity exercises, including the congressionally-mandated TOPOFF exercises. Additionally, our ISAC represented FSSCC in *Cyber Storm* and *Cyber Tempest*, two exercises focused on cyber-related issues. Our ISAC is also helping to plan *Cyber Storm II* which is scheduled for March 2008. FSSCC believes exercise participation is critical, and we encourage exercise planners to include our sector during the planning phases of their exercises.

PCIS Working Group

FSSCC has also been an active participant in the Partnership for Critical Infrastructure Security (PCIS), and I am a member of the Executive Committee and Board of PCIS. PCIS has a working group focused on cross-sector collaboration of cybersecurity issues. FSSCC's active participation in PCIS helps address cross-sector interdependencies and is an example of the collaborative model being used to build a strong cybersecurity network.

Future Challenges

Many cyber security initiatives are on-going, and there are still several issues to address. Two issues relate to the GAO's SSP report and the DHS' R&D budget.

GAO Report

According to GAO, the Banking and Finance Sector's SSP is "somewhat comprehensive" in addressing cybersecurity. Because the GAO didn't consult with the Treasury or FSSCC when preparing their report, I respectfully disagree with their conclusions.

Our SSP, including the *Research Challenges* document, adequately addresses the GAO's criteria for cybersecurity R&D. For example, the R&D Committee is identified as the primary mechanism to solicit information on R&D initiatives, and their *Research Challenges* report details the sector's goals and gaps related to cybersecurity. Examples

in the SSP and in my written testimony contradict GAO's finding that we failed to identify programs to detect, deter, respond and recover from cyber attacks. The GAO report stated our SSP failed to describe a process for investment priorities, but our R&D's *Research Challenges* and the *Research Agenda* reports highlight a number of priorities where investment dollars could be directed. Without further guidance from GAO it's unclear how they reached their conclusions. We welcome a dialogue with GAO on these issues.

SSC/SSA R&D Budget

Finally, FSSCC believes DHS should consult with the private sector coordinating councils, and, at the very least, their sector specific agencies, on research project funding.

FSSCC thinks it makes good economic sense to fund programs supporting the R&D priorities developed by our industry experts. To achieve this goal, greater communication and consultation is necessary among DHS, Treasury and FSSCC. Another option would be to provide direct grant authority to the SSAs. Currently, FSSCC can only influence R&D project funding through its support letters.

In short, FSSCC believes the DHS cybersecurity R&D budget should be more closely aligned with the level of threat posed. An appropriation of only twelve million dollars is clearly insufficient. Our nation would be better served by providing additional budget discretion and dollars to projects identified by the industry under attack.

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