Statement for the Record
of
Greg Schaffer
Acting Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Committee on Financial Services,
Subcommittee on Financial Institutions and Consumer Credit
Washington, DC

September 14, 2011

Introduction

Chairwoman Capito, Vice Chairman Renacci, Ranking Member Maloney, and distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission with a particular focus on efforts to reduce cybersecurity risks posed to the Banking and Finance Sector.

Cybersecurity threats to critical infrastructure and services endanger their confidentiality, integrity and availability. DHS, working with our federal partners, assists the private sector in countering these threats and mitigating vulnerabilities in critical systems. This mission is especially critical to the financial sector in today's climate of growing economic and national security concerns. The Department is committed to working more closely with this subcommittee to reduce risk across the Banking and Finance Sector while increasing our cybersecurity posture. To achieve our shared goals, we need to increase the sharing of timely and relevant intelligence information concerning cybersecurity threats with financial sector stakeholders while increasing public awareness of the important role cybersecurity plays in ensuring safe and reliable banking and financial services.

The Current Cybersecurity Environment in the Banking and Finance Sector

The Banking and Finance Sector provides critical deposit, consumer credit, and payment processing services that have become integral aspects of everyday life. As with other U.S. critical infrastructure sectors, financial institutions face a combination of known and unknown vulnerabilities, including the expansion of adversaries' capabilities and challenges to threat and vulnerability awareness. Because financial institutions are critical to the Nation's economic security and handle large sums of money, malicious actors find them to be especially attractive targets. There are also risk considerations associated with the Banking and Finance Sector's dependencies on other critical infrastructure sectors. In simple terms, financial transactions would be significantly impacted by massive power outages or failures of U.S. communications services. In addition to providing regular updates on the latest threat mitigation techniques, DHS released the *Banking and Finance Sector Specific Plan*[1] in 2007, which characterizes

[1] http://www.dhs.gov/files/programs/gc_1179866197607.shtm

vulnerabilities associated with links between financial institutions and other sectors while offering sector-specific risk considerations.

Though malicious cyber actors have varying levels of access and technical sophistication, all seek to inappropriately leverage the systems they target. Analysis of criminal activities shows increasing levels of sophistication in technical and targeting capabilities as well as a willingness to sell these capabilities on the black market. Some adversaries are capable of disrupting, destroying, or exploiting U.S. information systems including those that support the Banking and Finance Sector while others pursue intelligence collection, intellectual-property theft, monetary theft, and the disruption of commercial activities. In response to these growing and persistent threats, the Banking and Finance Sector has developed sophisticated tools and frameworks to defend against, detect, respond to, and mitigate cyber threats in collaboration with other stakeholders, including IT sector companies and experts who often provide these capabilities to the financial sector.

Additionally, the Federal government's unique expertise and ability to coordinate analytical and response activities among government, law enforcement, and the intelligence community complements the Banking and Finance Sector's efforts. Based on the framework established by the *National Infrastructure Protection Plan (NIPP)*, DHS collaborates with the U.S. Department of the Treasury (Treasury) as the Sector-Specific Agency for the Banking and Finance Sector, the Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and other industry and interagency partners to reduce the risks posed to the critical systems that support the Nation's financial institutions. DHS also offers direct assistance to individual companies by assisting in analysis and improving their cybersecurity posture in addition to responding to requests for assistance from companies who have been compromised.

Despite significant outreach and relationship building, DHS faces a number of constraints in coordinating with the private sector, which may impact work with financial institutions. Some institutions have concerns about the privacy implications of sharing information with the Government or about brand damage that may result from reporting an incident. Through trusted relationships with financial sector institutions, including the Protected Critical Infrastructure Information program, DHS works to prevent inappropriate disclosure of proprietary information or other sensitive data. Furthermore, the Administration's cybersecurity legislative proposal offers a chance to provide clear statutory authority to facilitate greater information sharing between DHS and the private sector.

DHS Cybersecurity Mission

No single technology or government entity can overcome the cybersecurity challenges the Nation faces on its own. The public and private sectors must work collaboratively to address the risks posed to our Nation's critical systems.

At DHS's National Protection and Programs Directorate (NPPD), in addition to leading the effort to secure Federal Executive Branch civilian agencies' unclassified networks, we are responsible for several other cybersecurity missions, including:

- Providing technical expertise to the private sector and to critical infrastructure owners and operators, including at the state and local levels, in order to enhance their cybersecurity preparedness and broaden their risk assessment, mitigation, and incident response capabilities;
- Raising public cybersecurity awareness; and
- Coordinating the national mitigation response to cyber incidents.

In 2009, President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) and its associated cyber activities should remain a priority for the federal government. Consistent with the CNCI's priorities, the President's *Cyberspace Policy Review* established a strategic framework for advancing the Nation's cybersecurity policies. Following the May 2009 publication of this review, DHS designated safeguarding and securing cyberspace as a priority mission area in the Quadrennial Homeland Security Review (QHSR). To execute on this mission area, DHS established the following two overarching goals:

- Creation of a safe, secure, and resilient cyber environment and
- Promotion of cybersecurity knowledge and innovation.

Within NPPD, the Office of Cybersecurity and Communications (CS&C) focuses on reducing the risks posed to communications and information technology infrastructures, and to the sectors that depend on those infrastructures. CS&C also seeks to enable timely response and recovery of these infrastructures in all circumstances while coordinating information sharing efforts among Federal law enforcement, intelligence, defense, and homeland security communities to ensure a common operating picture of the cybersecurity and communications environment. Three divisions make up CS&C: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System. In addition, CS&C established the National Cybersecurity and Communications Integration Center (NCCIC), which coordinates interagency mitigation response efforts in the event of a significant cybersecurity incident.

Consistent with its role in implementing the NIPP, NCSD collaborates with the Banking and Finance Sector to conduct risk assessments and mitigate vulnerabilities and threats capable of affecting the sector's information technology assets and critical infrastructure. NCSD's Cyber Security Evaluations Program conducts Cyber Resilience Reviews to proactively determine how various organizations manage the cybersecurity of significant information services and assets while offering guidance to improve cybersecurity management and reduce operational risks related to cybersecurity. In doing so, NCSD carries out the majority of DHS's non-law enforcement cybersecurity responsibilities within the financial services sector.

One of NCSD's operational arms, the U.S. Computer Emergency Readiness Team (US-CERT), works closely with banking and finance sector partners to provide analytical expertise and to share threat and vulnerability information in collaboration with other critical infrastructure sectors, law enforcement, and the intelligence community. Through the FS-ISAC, the Banking and Finance Sector provides US-CERT with threat, incident, and vulnerability data, which is then integrated into US-CERT's analytical and information sharing processes.

NCSD's Critical Infrastructure Cyber Protection & Awareness (CICPA) branch builds on this effort by providing security clearances to key cybersecurity officials within the Banking and Finance Sector. For example, DHS has sponsored Top Secret/SCI clearances for select members of the financial services sector and numerous Secret-level clearances in partnership with Treasury to broaden the scope of information that US-CERT can share. US-CERT has also benefits from close operational collaboration with DHS's U.S. Secret Service Criminal Investigative Division (USSS-CID), which has concurrent jurisdiction with the FBI over the investigation of computer crime and protects the Nation's financial payment systems while combating transnational financial crimes committed by terrorists and other criminals.

Research and Innovation

In addition to NPPD's cybersecurity activities, the DHS Science & Technology (S&T) Directorate is closely engaged with the Financial Services Sector. One of the many innovations emerging from S&T's partnership with the Financial Service Sector is the Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE) software suite. DECIDE will enable enterprise decision makers to evaluate responses to operational disruptions of market-based transactions across networks. This allows stakeholders to pursue effective business continuity practices that address increasingly sophisticated cyber threats. DHS Science & Technology (S&T) Directorate is closely engaged with the FSSCC to develop capabilities to protect citizens by enhancing the resilience, security, integrity, and accessibility of information systems used by financial institutions and other critical infrastructures. In December 2010, S&T signed a memorandum of understanding with the FSSCC and the National Institute of Standards and Technology (NIST) to expedite the coordinated development and availability of collaborative research, development, and testing activities for cybersecurity technologies and processes.

Interagency and Sector Coordination

The success of our efforts to reduce cybersecurity risks posed to the Banking and Finance Sector depends on effective communication and critical partnerships. No single entity has sole responsibility for securing cyberspace. To that end DHS works with its Federal partners to host a number of initiatives focused on enhancing coordination and information sharing with the private sector.

Private Sector Security Clearance Program

The NCCIC maintains a program that hosts Top Secret/SCI-cleared private sector representatives on the NCCIC operations floor including representatives from the FS-ISAC. This program was created to closely integrate the operational capabilities of the NCCIC, various critical infrastructure sectors, and individual companies. The FS-ISAC's presence on the NCCIC floor enhances the analysis, warning, and response capabilities associated with critical information systems and improves the overall cybersecurity of the Banking and Finance Sector and the Nation.

Cybersecurity Information Sharing and Collaboration Program

In February 2010, DHS, the Department of Defense, and the FS-ISAC launched a pilot designed to help protect key critical networks and infrastructure within the Banking and Finance Sector by sharing actionable information. Based on knowledge gained from the pilot, DHS is expanding

its information sharing and incident response coordination processes with other critical infrastructure sectors and leveraging capabilities from within DHS and across the response community. Specifically, DHS plans to launch the critical infrastructure Cybersecurity Information Sharing and Collaboration Program this year, which seeks to create a secure online collaboration portal where registered critical infrastructure sector entities can provide accurate, timely, and thorough information about current, emerging, and evolving threats posed to critical infrastructure networks. The portal will have the capability to process Protected Critical Infrastructure Information while offering timely and actionable analysis and mitigation products for critical infrastructure participants based on stakeholder contributions and unclassified government reporting.

Cyber Operations Resiliency Review Pilot Program

In addition, NCSD, in partnership with Treasury and the BITS Financial Services Roundtable, is implementing a two-phase pilot program to proactively assess the degree of cyber resilience and presence of malicious activity on up to five financial institutions' enterprise networks. In the first phase, analysts from CICPA's Cybersecurity Evaluation Program will measure the adoption and growth of cybersecurity risk management using a common capability-based evaluation framework. In the second phase, US-CERT will analyze institution-provided data for evidence of malicious activity. If malicious activity is found, US-CERT will provide the institution with targeted strategies to mitigate the activity and protect against similar activity in the future.

National Cyber Incident Response

The President's *Cyberspace Policy Review* called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." To address this presidential priority, DHS created a working group of stakeholders from the public and private sectors that drafted the *National Cyber Incident Response Plan* (NCIRP). The NCIRP provides a framework for the NCCIC's response capabilities and for coordination of Federal, state and local governments, the private sector, and international partners during significant cyber incidents. The plan specifically addresses the role of the Treasury and the FS-ISAC in providing for coordination of national response capabilities by providing flexible, adaptable synchronization of response activities across jurisdictional lines. In September 2010, DHS tested the NCIRP during a response exercise in which members of the domestic and international cyber incident response community addressed a scenario of a coordinated cyber event. The NCIRP working group is now completing the final stages of plan revision using observations from the exercise and experience from real world events.

National Strategy for Trusted Identities in Cyberspace

DHS also worked closely with our public and private sector partners on, the Administration's National Strategy for Trusted Identities in Cyberspace (NSTIC), which seeks to increase the security of online transactions through the development of more trustworthy digital credentials. The adoption of more trustworthy credentials will help to reduce account takeovers and raise overall consumer safety levels. Trusted identities are a key part of the Department's vision for a healthy cyber ecosystem. The voluntary adoption of credentials envisioned by the NSTIC will make online transactions faster, more convenient, safer and more private.

DHS Technical Assistance to the Banking and Finance Sector
Over the past year, DHS has demonstrated its ability to assist financial institutions with cyber intrusion mitigation and incident response while building on lessons learned. Initiating technical assistance with any private company to provide analysis and mitigation advice is a sensitive endeavor that requires trust and confidentiality.

In June 2010, for example, US-CERT partnered with the Federal Bureau of Investigation (FBI) to address a specific threat impacting a U.S. financial institution. By providing remote operational support following a formal request for technical assistance from the financial institution, US-CERT was able to analyze the threat, develop near-term mitigation recommendations, and identify strategies for preventing similar activity. In this instance, malicious actors used a combination of legitimate and illegitimate data to create false online accounts, ultimately giving them access to sensitive systems. A rapid cross-sector and interagency response effort prevented any known financial losses from this event.

As a result of knowledge gained during this engagement and from the collaborative relationship built with this particular financial institution, US-CERT was better able to assist another financial institution that experienced a similar event. In June 2011, US-CERT partnered with the Secret Service to assist the second institution with their detection and mitigation efforts and leveraged its relationship with the initial institution to bring the two entities together to discuss the vulnerability.

During an unrelated event in December 2010, US-CERT partnered with FBI and the National Security Agency to provide on-site and remote assistance and support in response to a significant cybersecurity incident involving financial entities. Upon formal request, US-CERT was able respond to this incident with specialized technical insight, support, and assistance. Specifically, US-CERT conducted interviews and briefings with high-ranking company officials, served as the lead for a skilled technical team of network analysts, and coordinated the development of a mitigation strategy with other agencies and financial sector institutions. Through our analysis and unique capability to coordinate cross-sector and interagency response efforts, we discovered other potential and actual victims of this threat. US-CERT aggressively worked to publish alert and awareness products for the wider community.

Of course, these are just two examples of how DHS works to achieve success in the analysis and warning mission space. We have proven our ability to earn stakeholder confidence when it comes to mitigating threats posed to networks, to reduce future risks, and to serve as the Federal government's focal point for analyzing incident reports.

Conclusion
The Nation's cybersecurity activities are set in an environment characterized by a combination of known and unknown vulnerabilities, rapidly expanding capabilities, and challenges in maintaining comprehensive threat and vulnerability awareness. The mission to reduce the cyber risks posed to the Banking and Finance Sector's critical systems is a national endeavor, requiring broad collaboration. Robust public-private approaches to cybersecurity are essential to ensuring that government, business, and the public can continue to use the critical services on which they depend. DHS is committed to working with its partners to create a safe, secure, and resilient

cyber environment that supports the Banking and Finance Sector and fosters national economic prosperity.

Thank you for the opportunity to discuss emerging issues in cybersecurity with you today and I am pleased to answer any questions you might have.