Statement for the Record
Gregory Garcia
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security
Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on
Emerging Threats, Cybersecurity and Science and Technology
and the Subcommittee on
Transportation Security and Infrastructure Protection
October 31, 2007

Good afternoon, Chairman Langevin, Chairwoman Jackson-Lee, Ranking Member McCaul, Ranking Member Lungren, and Members of the Subcommittees. Thank you for inviting me to speak about our efforts to work with all 17 critical infrastructure and key resource (CI/KR) sectors to address the security of the cyber elements of their infrastructures, including the incorporation of cyber security into their Sector-Specific Plans (SSP), progress in advancing mitigation actions, and plans for continuing to engage with the CI/KR sectors to further address cyber security.

One of the most pressing challenges facing the Department of Homeland Security (DHS) is preparing for cyber attacks against our CI/KR. Threats to the Nation's CI/KR are numerous and constantly evolving. The ability of threat actors to exploit vulnerabilities is facilitated by the widespread availability of tools, techniques, and information. A variety of cyber threats could exploit vulnerabilities in the Nation's CI/KR assets, systems, networks, and functions, potentially threatening national and economic security, public health and safety, and confidence in the government. The President's *National Strategy to Secure Cyberspace* recognized the importance of assessing threats and vulnerabilities and determining how likely or significant those attacks could be on critical infrastructure. It called for public-private partnerships to address five critical priorities: 1) a national cyberspace security response system, 2) a national cyberspace security threat and vulnerability reduction program, 3) a national cyberspace security awareness and training program, 4) securing governments' cyberspace, and 5) national security and international cyberspace security cooperation. The first three priorities speak directly to the development and implementation of the SSPs.

In implementing the *National Strategy* DHS' Office of Cybersecurity and Communications (CS&C), working in partnership with the Office of Infrastructure Protection (OIP), Sector-Specific Agencies (SSAs), and public- and private-sector security partners, is committed to preventing, preparing for, responding to, and recovering from cyber attacks and their consequences. CS&C's strategic goals include preparing for and deterring catastrophic incidents by achieving a collaborative risk management and deterrence capability with a mature partnership between government and the private sector. One example of this partnership is CS&C's National Coordinating Center (NCC). Since 1984, the NCC has served as a forum through which the Federal government and private sector communications providers can interact face-to-face on a daily basis. This strategic goal also encompasses tactical efforts to secure and protect the Nation's cyber infrastructure from attacks and disasters by identifying and mitigating threats, vulnerabilities, and consequences.

Our vision, philosophy, and strategy for preventing, responding to, and recovering from cyber attacks reflect the expanding and widespread importance of the cyber infrastructure. Policies that advance a safe and secure infrastructure rely on the valuable relationships between the public and private sectors and on public trust and confidence.

The key to continued success is partnering strategically with the private sector to identify, prioritize and protect critical cyber assets, systems, networks and functions. Even though the private sector builds, owns and operates most of the cyber infrastructure, CS&C takes an active role in its protection by building public-private partnerships that are vital to our strategy to secure cyberspace and to facilitating efforts to raise cyber security awareness, train personnel, stimulate market forces to secure cyberspace, improve technology through the identification of cyber research and development requirements, identify and remediate vulnerabilities, and exchange information.

CS&C works to reduce cyber risk and enhance cyber security in two primary ways under the National Infrastructure Protection Plan (NIPP) framework: 1) as Federal lead for the Information Technology (IT) Sector's infrastructure protection and preparedness responsibilities (in partnership with the Communications Sector); and 2) as a cross-sector cyber element that involves DHS, the SSAs for each of the 17 CI/KR sectors, and public and private sector owners and operators.

Homeland Security Presidential Directive 7 designates DHS as the SSA for both the Communications and IT sectors. CS&C's National Communications System (NCS) and the National Cyber Security Division (NCSD) carry out the SSA responsibility for the Communications and IT Sectors, respectively. Both sectors recently released their Sector Specific Plans (SSPs), which are planning documents that focus on overall sector preparedness, including managing risk to the sectors' critical functions and infrastructures that support homeland, economic, and national security. Under the NIPP framework, the Internet and its associated services are identified as a shared key resource of the IT and Communications Sectors, reflecting the convergence of voice and data communications networks and services. In their respective DHS-designated roles for the Communications and IT infrastructure sectors, the NCS and NCSD share responsibility with public- and private-sector security partners for the availability of the Internet and its associated services. Recognizing the synergies between IT and Communications, the chair of each sector's Government and Sector Coordinating Councils also participates in the other sector's council. In addition, representatives from the IT and communications sectors participate in each other's risk assessment methodology development efforts.

Cyber Security in the Sector-Specific Plans

In support of the cross-sector cyber responsibility, NCSD is working closely with OIP, the SSAs, and other security partners to integrate cyber security into the CI/KR sectors' protection and preparedness efforts.

During the SSP development process, NCSD provided cyber expertise to the sectors, including reviews of draft SSPs and participation in sector-specific cyber security meetings. Specifically, as sectors were developing their SSPs, NCSD developed and provided information to SSAs on resources for cyber security practices and protective programs that are applicable across all sectors, as well as some that are more focused on individual sectors, to help inform the identification of cyber security-related protective programs. For each protective program, a brief description and the specific activities they supported within the preparedness spectrum were provided. NCSD also developed information on cyber research and development (R&D) requirements and priorities to help SSAs in the identification of cyber-related R&D priorities. A description of Federal organizations that support cyber R&D and several references to R&D documents that outlined specific cyber security initiatives were provided. NCSD also offered to work directly with any sector that requested assistance and worked with responding sectors to develop and review cyber security content for the SSPs.

NCSD also developed a comprehensive SSP Cyber Guidance Checklist, which provided sectors with a framework for integrating cyber security throughout each section of their SSPs. The checklist complemented DHS' 2006 CI/KR Protection SSP Guidance developed by OIP and was intended to provide a starting point for SSAs as they integrated cyber into their SSPs. The checklist included an outline and guidance for the development of cyber content for the SSPs. NCSD shared the checklist in OIP-sponsored technical assistance sessions with SSAs to provide expertise and answer questions regarding the inclusion of cyber security in the SSPs. NCSD personnel also met individually with those SSA representatives who expressed an interest in determining approaches for incorporating cyber security into their SSPs and sector risk management efforts.

In December 2006 and January 2007, NCSD conducted a review of the final draft SSPs as part of OIP's review process to 1) assess each sector's plan for securing its cyber infrastructure and 2) understand the coordination between NCSD and the sectors needed to better secure the sector's cyber infrastructure. In addition to considering the full content of the SSPs, this review focused on specific areas where future coordination between NCSD and the sectors might be necessary to address the security of the cyber elements of the Nation's CI/KR, including the critical initial action to identify the sectors' cyber security partners that NCSD should engage with to manage cyber risk. NCSD also determined that coordination may be required in understanding how each sector plans to identify and assess risk to its cyber infrastructure. Coordination is also required when assisting sectors in the development or refinement of methodologies intended to identify critical cyber elements and to assess cyber risk. Finally, the review identified protective programs specific to cyber security that fall within NCSD's responsibility and cyber R&D priorities requiring coordination across the sectors and with DHS' Science and Technology Directorate.

After the SSPs were finalized, NCSD conducted a second review of the documents on behalf of the Cross-Sector Cyber Security Working Group (CSCSWG). The CSCSWG provides a forum for exchanging information on common cyber security challenges and issues (i.e., threats, vulnerabilities, and consequences) and enhancing the understanding across sectors of mutual dependencies and interdependencies. The working group includes cyber security experts from the CI/KR sectors collaborating to identify systemic cyber risks and mitigation strategies for the Nation's CI/KR sectors. The CSCSWG held its inaugural meeting on May 30, 2007, and determined that an initial area of focus would be reviewing the cyber security components of the SSPs to better understand the various efforts to protect cyber elements of the 17 CI/KR sectors and identify trends in cyber infrastructure protection that cut across the sectors. Using the NCSD review as a starting point, the group provided input on sectors' cyber content and on cyber activities not fully captured or initiated after the drafting process. The group has begun to share successes, best practices, and lessons learned to help the development and implementation of more effective cyber risk management activities across the sectors. For example, through the CSCSWG, members learned about the Roadmap to Secure Control Systems in the Energy Sector. As a result, the Water and Chemical Sectors have chosen to initiate similar efforts to address the unique concerns of control systems security within their sectors.

Progress in Advancing Mitigation Actions

Many of the SSPs were created in summer and fall of 2006. Sectors have been implementing the plans, continuing or initiating efforts to address the security of their cyber infrastructure. Sectors are not uniformly comprehensive in their cyber security efforts and should not necessarily be. Each sector must consider its cyber security posture and balance that against other risk management efforts, in consideration of the unique aspects of its infrastructure. Cyber risk varies by sector, based on its dependence on cyber elements. For example, the extensive use of control systems in the Energy Sector and of business systems in the Financial Services Sector must factor into the extent, sophistication, and unique implementation of mitigation and protection strategies within those sectors. Other sectors do not have cyber infrastructure integrated as ubiquitously in their essential services, a fact that influences the focus and maturity of their cyber security efforts. The length of time a sector's public and private partners have been working together on infrastructure protection issues is another factor in the comprehensiveness of their plans. These observations regarding the cyber security position of the SSPs are generally consistent with the findings of the Government Accountability Office's (GAO) analysis.

The integration and maturing nature of cyber security across the 17 CI/KR sectors was clear when NCSD reviewed and contributed to the Sector Annual Reports (SARs). The sectors' 2007 SARs were much improved over their initial 2006 efforts. For example, more than half of the sectors identified at least one cyber security goal and/or priority in their second SAR. This represents a significant increase in the number of sectors from the 2006 SAR, suggesting that the understanding of the importance of cyber security is becoming more pervasive in the sectors.

Further, more sectors are implementing DHS-sponsored protective measures, such as the Comprehensive Review, the Risk Analysis and Management for Critical Asset Protection (RAMCAP), and the Site Assistance Visit programs. NCSD collaborates with OIP to incorporate cyber security into these DHS risk and vulnerability assessment programs so that sectors implementing them would address the cyber elements of their infrastructure. We encourage sectors to assess cyber risk by using the Cyber Security Vulnerability Assessment (CSVA), a flexible and scalable approach that analyzes an entity's cyber security posture and describes gaps and targeted considerations that can reduce overall cyber risks. It assesses the policies, plans, and procedures in place to reduce cyber vulnerability in 10 categories (e.g., access control, configuration management, physical security of cyber assets, etc.) and leverages various recognized standards, guidance, and methodologies (e.g., International Organisation for Standardization 27001, Information Systems Audit and Control Association Control Objects for Information and related Technology, and the National Institute of Standards and Technology Special Publication 800 series). The CSVA tool is being used by six sectors in their tailored vulnerability assessments: five through their sector specific RAMCAP modules and another, the Transportation Sector, in its customized cyber security assessment.

Plans for Continuing to Engage with the CI/KR Sectors to Further Address Cyber Security

Our review of the SSPs and SARs found that sectors are paying attention to cyber security, but more needs to be done. Over the next year, sectors need to focus on identifying their critical cyber infrastructure, assessing cyber risk and promoting voluntary assessments, implementing protective programs, and measuring the effectiveness of their efforts.

NCSD has created an action plan and is engaging with sectors in addressing cyber security issues not fully addressed in those sectors' initial SSPs. This action plan includes working with sectors to review cyber security priorities, assess effects of cyber attacks, develop protective programs, and evaluate R&D requirements and initiatives to identify areas where additional capabilities are needed. NCSD has already worked with the cyber experts of the Chemical Sector Coordinating Council (SCC) and the SSA to identify cyber security content needed for the 2008 update to their SSP. Some of the opportunities for engagement are based on sector specific needs, but others address more common challenges. The action plan will address both individual and more universal steps.

While all sectors have established SCCs and Government Coordinating Councils (GCCs), the degree of examination of specific cyber risk and of cyber information sharing varies. Some sectors – such as Financial Services – consider cyber security as critical to their core business functions and integrate cyber security into all of their SSP implementation activities. In fact, the Financial Services SSA, the Department of the Treasury, sits on the IT GCC because of its interest and expertise in cyber security. Other sectors have historically had less focus on cyber security due to the lack of prominence of IT in the business of the sector. Representation from the sectors' SCCs and GCCs are participating in the CSCSWG provides a mechanism for two-way information flow on cyber concerns across all sectors. Participation in the CSCSWG may help less-mature sectors make more rapid progress in identifying cyber goals, gaps, and interdependencies, as well as developing programs to deter, respond and recover from cyber attacks by enabling them to leverage the experiences, work, and cyber functional expertise that exists in many sectors.

In addition, the reliance of some sectors on control systems highlights an area for increased coordination of risk management efforts. NCSD's Control Systems Security Program (CSSP) and the Process Control Systems Forum (PCSF) are resources to help address control systems risk. The CSSP coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors, to improve control system security within and across all critical infrastructure sectors. In support of risk mitigation efforts, the CSSP developed the Control Systems Cyber Security Self Assessment Tool and provides training in control systems cyber security. The PCSF, a standing group under the CSCSWG, works to develop solutions for process control systems security, aggregate information, connect decision makers, and leverage other groups' work.

Sectors may leverage the United States Computer Emergency Readiness Team (US-CERT) to share information on cyber threats and vulnerabilities and enhance situational awareness. The timely detection and analysis of cyber attacks further helps to assess operational risk and mitigate the impact on our Nation's critical infrastructures of cyber vulnerabilities. US-CERT is working with the Information Sharing and Analysis Center Council to expand this operational interaction.

Finally, most sectors are taking on the challenge of identifying or developing metrics to measure the effectiveness of all infrastructure protection efforts, including those for cyber. Since sectors have different overall approaches to infrastructure identification and risk management, NCSD will work with the sectors to develop some cross-sector qualitative measures that correlate to cyber security to help measure the effectiveness of sectors' cyber security efforts.

Conclusion

The development of the 17 CI/KR SSPs represented a significant milestone in sectors' protection and preparedness activities. Sectors varied in how they addressed the security of the cyber elements of their infrastructures, including the incorporation of cyber security into their SSPs, but demonstrated increased understanding of the importance of cyber security in the SARs and implementation activities.

As the sectors work to address the feedback from the GAO on the cyber security aspects of the SSPs, CS&C, and specifically, NCSD will continue to execute its cross-sector cyber responsibility to work with sectors to reduce cyber risk and enhance cyber security. Our goal is to create a clear and actionable path forward with the sectors and to work together to secure our critical cyber infrastructure.

NCSD will continue to schedule regular interactions with individual sectors as well as meetings with multiple sectors. For example, we plan to meet with each SSA at least twice a year, once before the sectors update their SSPs and once in early spring of 2008 as sectors are preparing their SARs. NCSD will develop guidance on cyber elements that should be considered for inclusion in the SSPs and SARs. This guidance will complement guidance from the Office of Infrastructure Protection. NCSD will also work with sectors through their coordinating councils to identify cyber subject matter experts within their sectors and raise awareness of the sectors' reliance on cyber infrastructure. NCSD is piloting this approach by convening a small group of cyber security experts with security clearances from across the sectors to support the SSA risk assessment process for the 2008 National CI/KR Protection Annual Report.

NCSD also plans to offer workshops in 2008 with sector partners and other invited subject matter experts to address incentives to encourage voluntary risk assessments, develop cross-sector cyber metrics, and identify existing cyber research and development projects. The outcome of these workshops will provide sectors with ideas for incentives for investing in cyber security, metrics that enable realistic evaluation of cyber security, and cyber R&D priorities. NCSD will also continue to support the efforts of the CSCSWG as it addresses opportunities to enhance cyber security across the sectors and share information about strong cyber programs and practices. Further, NCSD will continue to roll out important efforts like the CSVA, software assurance, and control systems acquisition guidance, training, and cyber exercises to our sector partners.

We encourage sectors to continue to work collaboratively with NCSD on addressing cyber security in their infrastructure protection activities. Through participation in the CSCSWG, individual meetings with NCSD, and various NCSD-sponsored workshops and programs, sectors can make significant progress in the future to address or more fully address cyber security.

We must reinforce a culture of preparedness, shift from a reactive to a proactive stance, and prepare by promoting effective cyber security strategies that evolve as the risks evolve. There is much work to be done, but progress continues every day. We rely on the support and expertise of the sectors to advance this mission.

I would like to thank the Subcommittees for their time today, and I appreciate this opportunity to discuss these important cyber security priorities.