PRIVATE-SECTOR PREPAREDNESS

IN CRITICAL INFRASTRUCTURE PROTECTION

Testimony of
Kenneth C. Watson
Vice Chairman, Partnership for Critical Infrastructure Security, Inc. (PCIS)

To
U.S. Senate
Senate Homeland Security and Government Affairs Committee
Ad Hoc Committee on State, Local and Private Sector Preparedness and Integration

Washington, D.C.
July 12, 2007

Mr. Chairman and Members of the Subcommittee:

I am Ken Watson, Manager of Cisco's Critical Infrastructure Assurance Group. I am here today in my capacity as the elected Vice Chairman of the Partnership for Critical Infrastructure Security (PCIS). Thank you for inviting the PCIS to participate in today's hearing on America's private-sector preparedness to protect our critical infrastructure. I believe the nation's critical infrastructures and key resources represent the new "center of gravity" for defending our national and economic security. The companies and associations that constitute the membership of PCIS are eager to continue doing their part to ensure the ongoing delivery of critical infrastructure services on which the nation and its citizens depend for just about everything we do, day in and day out.

The increasingly interconnected nature of the world's economy has created a global marketplace of ideas and commerce. Every industry in the United States, and throughout the developed world, is increasingly dependent on every other. The Federal government relies on the services provided by private-sector infrastructure owners and operators. Many of these owners and operators lead multinational corporations, and all have an interlaced global network of suppliers, partners, and customers. The health of this networked global economy is directly relevant to the health of America's national and economic security.

The National Infrastructure Protection Plan (NIPP) designates the PCIS as the private-sector cross-sector coordinating council for protecting critical infrastructure. Our council consists of the Sector Coordinating Councils (SCCs) for all the critical infrastructure sectors designated in Homeland Security Presidential Directive-7 (HSPD-7) that have private-sector components. (The Government Facilities and National Monuments and Icons sectors do not have private-sector components). The strength of the PCIS is generated by the expertise and leadership found in those SCCs. In turn, SCCs reflect the make-up of the key companies and leaders in the sectors. Most of the sectors have also established Information Sharing and Analysis Centers (ISACs) to manage their day-to-day information sharing needs. As I discuss progress and perspectives of the sectors, I will underscore the roles of the SCCs and the ISACs.

In response to a call for public-private partnership from the Federal government, several private-sector critical infrastructure owners and operators founded PCIS in 1999. That call was itself a response to the October 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP), "Critical Foundations," led by retired General Robert Marsh. Because of what it characterized as two irreversible trends, the Marsh Commission found that a strong public-private partnership was the only path to secure infrastructures. Those two trends—increasing privatization of critical services and increasing migration of core business and government operations to networks, including the Internet—continue today. Government can no longer defend the country by itself—it has neither the specialized expertise nor the network access required.

The private sector has not organized itself neatly into departments and agencies as the government has. Therefore, there were unique challenges in constructing an architecture that not only reached the right expertise in each sector, but also provided for universal access for all sector members. Moreover, the framework would need to include a robust, multi-level information-sharing mechanism that could reach executives and experts in a timely manner. Not

surprisingly, the first attempts at building this partnership had mixed success—on both the public and private-sector sides of the partnership. Nevertheless, after eight years of hard work, we have made tremendous progress. It is not perfect, but I believe we are on a very solid path, and the United States is far more resilient to potential attacks or natural disasters affecting critical infrastructures than it was eight years ago.

Today, I will provide an overview of PCIS goals, present examples of recent progress, offer benchmarks for continued success, address some specific concerns and perspectives of the sectors, and discuss joint industry-DHS initiatives to remove barriers to private-sector participation in the partnership. Finally, I will offer suggestions regarding what the government might do to continue strengthening this partnership and improving our resilience in both physical and cyber security.

When we created PCIS, we envisioned it as a cross-sector coordination mechanism for policy and strategy matters, neither operational nor authoritative in its own right. SCCs are the resident experts from the sectors, and therefore we defer to that expertise for specific questions regarding sector operations. The PCIS mission is to "coordinate cross-sector initiatives that promote public and private efforts to ensure secure, safe, and reliable critical infrastructure services." This overall goal continues today. This past April, we published our first comprehensive business plan, which covers the three-year period 2007 to 2009. I have attached it to my written testimony for your reference.

The business plan outlines PCIS objectives, products and services, strategies for communications, organization, management, operations, research and development, and support, and it provides details on our current working groups and committees. Our members tell us they see value in understanding issues common to multiple sectors, unique challenges or solutions from a single sector, and the ability to jointly approach DHS and other government organizations.

Primarily, PCIS seeks to improve continuously the overall national capability to ensure critical infrastructure services and protect supporting critical assets and functions. We accomplish our mission by fulfilling the following roles:

- Address physical, cyber, and human cross-sector critical infrastructure protection and interdependency issues of concern to sector owners and operators;
- Improve the security and safety of the nation's critical infrastructures by enabling critical infrastructure sectors to collaborate among themselves, as well as in partnership with governments;
- Encourage and participate in productive public-private partnerships with government as enabled by the Critical Infrastructure Partnership Advisory Council (CIPAC);
- Participate in CIPAC (through PCIS members); and
- Serve as the Private-Sector Cross-Sector Council in the NIPP Sector Partnership Framework.

PCIS is guided by three core principles:

1. *Build effective collaborative relationships between the sectors and government by improving coordination, cooperation and communication.*
2. *Promote a comprehensive approach to detect, prepare, prevent, protect, respond and recover from all threats and hazards that may cause incidents of national significance.*
3. *Promote the merits of a non-regulatory approach to advance the security and resilience of the sectors.*

The PCIS business plan identifies four broad goals, each with subordinate objectives and metrics.

1. Partnership Leadership for all-sector critical infrastructure protection issues and policy;
2. Cross-Sector Leadership for cross-sector and interdependency issues;
3. Sector Assistance for healthy and productive partnership interactions; and
4. PCIS Effectiveness for strong organizational effectiveness and value.

In addition, because of the comprehensive, sector-specific subject-matter expertise resident in PCIS, the National Infrastructure Advisory Council (NIAC) calls on us from time to time as it develops policy advice for the President. Two notable recent efforts were:

- Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States; and
- Public-Private Sector Intelligence Coordination.

There are numerous examples of recent successes. Chief among those is development of the NIPP and its 17 Sector-Specific Plans (SSPs). The level of collaboration we enjoyed would have been impossible without the CIPAC framework provided by the Congress in the Homeland Security Act of 2002 and implemented by Secretary Chertoff more than a year ago. CIPAC represents a partnership between government and critical infrastructure/key resource (CI/KR) owners and operators. The Council provides a forum in which these partners can engage, freely and openly, in a broad spectrum of activities to support and coordinate critical infrastructure protection. The CIPAC framework allowed us to roll up our sleeves and work side-by-side with our government counterparts to write these plans.

One significant result of this collaboration is the NIPP's approach to risk management. Before private-sector participation began, the draft proposed a bottom-up approach, which focused on physical assets. But after considerable engagement between DHS and sectors that are less dependent on specific physical assets than on functional systems (such as electric power, communications, and information technology), the NIPP risk management section evolved to accommodate top-down, functionally-based risk management models, permitting these multiple approaches.

The incorporation of the top-down, functional approach reshaped the NIPP into a useful framework for all the SSPs, not just for those with a finite number of discrete physical assets. Rather than using taxpayer funds to develop border-zone protections for these sectors, the NIPP framework will eventually identify smarter ways to spend Federal resources. One example of a sector with a top-down, functional approach can be found in the Communications Sector.

- Communications—Communications networks are dynamic; the most important assets change depending on the circumstances. Some of the most important assets may be the people assigned by companies to the National Coordinating Center for Telecommunications. They work with each other under mutual support agreements, coordinating closely with 23 Federal agencies on day-to-day incidents, including everything from backhoe cable cuts to Denial of Service (DoS) attacks against carriers.

Developing the SSPs was not a perfect process. Not all Sector-Specific Agencies (SSAs) worked as closely with their private-sector counterparts as others. Most sectors were very pleased with their collaboration, but for others a learning curve remains. I see these as growing pains as both government and owner-operators embrace the new partnership framework.

I am happy to report the list of sector successes is a long one, and growing by the day. So now, I would like to mention six success stories, each one of which is representative of the tremendous work and progress all of our critical infrastructure sectors are making.

- Financial Services—In 2003, 14 Chicago-area financial institutions formed a nonprofit organization called ChicagoFIRST, which they designed to address homeland security and emergency management issues requiring a coordinated response with all levels of government. Today, ChicagoFIRST is 26 members strong, and growing. The group collaborates daily with the City of Chicago, State of Illinois, and numerous Federal agencies on disaster management matters. Since it was founded, ChicagoFIRST has obtained a seat in the Chicago emergency operations center for the financial community, encouraged the city to implement a credentialing system, assisted in planning and executing an evacuation of four downtown skyscrapers, ensured that members receive important emergency information from government, and worked with the city and State on pandemic preparedness. Now, similar regional partnerships are forming, using ChicagoFIRST as a model. A new informal organization, RPC FIRST (Regional Partnership Council for Financial Industry Resilience, Security, and Teamwork) shares best practices, solicits advice, and participates in the national Financial Services Sector Coordinating Council (FSSCC).
- Rail and Water—The Association of American Railroads (AAR) is working with three ISACs, which meet quarterly with intelligence personnel from DHS, FBI, CIA, National Security Agency, and the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network to add realism and usefulness to quarterly industry threat assessments. These meetings have enhanced mutual trust, increased knowledge of cross-sector dependencies, and raised understanding among government analysts of rail industry operational characteristics. In addition, the WaterISAC, managed by the Association of Metropolitan Water Agencies, also conducts quarterly meetings with intelligence personnel from DHS, FBI, and others to crosscheck the Sector's intelligence gathering efforts with those of the Federal intelligence community.
- Dams—In addition to holding classified briefings and establishing a Dams portal on the Homeland Security Information Network (HSIN), the Dams Sector has developed a close working relationship with the DHS National Cyber Security Division (NCSD). The Dams Sector assists DHS and the Federal Energy Regulatory Commission (FERC) conduct annual security seminars for the FERC-regulated Sector members. To educate owners of smaller dams about current and future security initiatives as well as assessments of threats, the Dams Sector draws on the expertise of various member associations.

- Water—The American Water Works Association (AWWA), with support from the Environmental Protection Agency (EPA) and other Sector associations, has been leading an initiative to support the development of intrastate mutual aid and assistance networks between water and wastewater utilities (public and private) to increase the Sector's preparedness and response capability to natural and man-made incidents. For the past year, the Sector has put on workshops to introduce the concept and develop action plans. Currently there are nine Water/Wastewater Agency Response Network (WARN) states, and more than 30 states are currently establishing a WARN program.
- Commercial Facilities—The International Association of Assembly Managers (IAAM) used a DHS Competitive Training Grant to create a six-hour training course to assist in promoting and training facility managers on the Vulnerability Identification Self-Assessment Tool (ViSAT). DHS developed ViSAT, a Web-based tool, to enable asset owners and operators to provide security awareness training and to conduct voluntary vulnerability assessments of their facilities. Within the Commercial Facilities Sector, modules have been programmed into the system for stadiums, arenas, performing arts centers, and convention centers. IAAM has identified between 12 and 15 locations in the public assembly community to roll out the ViSAT training program.
- Nuclear—The Nuclear Sector represents all 104 operating U.S. nuclear power reactors, research and test reactors, and the radioisotope community. It formed in late 2004, and, in a short period, worked collaboratively with DHS to develop and implement the Risk Analysis and Management for Critical Asset Protection (RAMCAP) and Comprehensive Review (CR) processes. By the end of this year, RAMCAPs and CRs will be completed at all operating nuclear power reactors in the United States. Most importantly, insights from CRs have led to actions taken by plant owners and emergency responders (Federal, State, and local) that have made significant improvements to the security posture and responsive capabilities for those key resources. Further, with DHS, the Nuclear Sector completed initial planning for pandemic flu preparedness by early 2006, and has advanced that effort within the Sector and worked outside the Nuclear Sector to help more broadly. Moreover, in several specific intelligence and technical areas, the Sector has worked very closely with the Department of Homeland Security (DHS) in a manner that has led to measurable improvement in the security of our nuclear power plants.

Removing any perceived or actual barriers to private-sector participation is a key initiative of DHS, as well as the PCIS. In your invitation, the Subcommittee asked me to comment on three areas of concern today:

1. Issues of competitive advantage;
2. Fear of sharing sensitive information; and
3. Worries the partnership might exclude smaller operators.

Regarding competition, a quote by Gregg Jones in a recent Business Executives for National Security (BENS) report, "Getting Down To Business," reflects the way PCIS operates. "We're competitors, not enemies," wrote Jones, the Chief Administrative Officer for Greenberg Traurig, LLP. "We collaborate during emergencies…" The same holds true for the SCCs and ISACs. I have seen this collaborative approach across all the sectors from the creation of PCIS through today, and I assure you these efforts are not merely about marketing or selling to customers.

Business works with our government partners to develop policies, strategies, and information-sharing mechanisms we will all rely on during an emergency. ISACs, and their relationship to DHS, provide an excellent example of these non-competitive partnerships in action. Sectors that have ISACs use them to share information on threats, vulnerabilities, countermeasures, and best practices. ISACs coordinate regularly with each other and with the DHS U.S. Computer Emergency Readiness Team (US-CERT). PCIS is leveraging the ISAC Council (an *ad-hoc* coalition of the leadership of most of the industry ISACs) as it works with DHS on information-sharing policy issues.

Regarding sharing sensitive information, we are working closely with the Protected Critical Infrastructure Information (PCII) Program Office and the Information Sharing Environment (ISE) on two initiatives that would improve information sharing while also protecting sensitive information. The President tasked the ISE to reform the classification criteria for "Sensitive But Unclassified" (SBU) information. Under the CIPAC framework, PCIS members are working with ISE and DHS personnel to develop a simplified, rational approach to protecting information. Most recently, the ISE combined our latest comments with those of Federal departments and agencies in a draft guideline document that is on its way to a Principals Committee review. As long as statutory protections (for CII) remain in place, the PCII program should function within the newly proposed "Controlled Unclassified Information" (CUI) environment. Despite these efforts, some sectors continue to have serious concerns for two primary reasons. First, sectors are unclear about what sensitive information DHS needs. Second, sectors remain concerned this information may be disclosed publicly, making it available to competitors or used in litigation.

In regards to including smaller operators, sectors have organized their SCCs to include all relevant trade and operational associations. This was a provision the private sector insisted upon, and DHS agreed to incorporate into CIPAC. An example of inclusion is the Food and Agriculture SCC, which has 119 separate entities representing all aspects of the Sector from "farm to table," including restaurants, grocery stores, meat packers, farmers, and food processors. Another is the Financial Services SCC, which has 34 associations and companies, representing banks, brokerages, and the insurance industry. Each SCC is aggressively pursuing ways to increase its reach, and I believe most of them are growing accordingly. In addition, Assistant Secretary Bob Stephan and others from DHS regularly travel around the country, conducting town hall-style meetings, where officials encourage companies and associations to join SCCs and ISACs.

Finally, please allow the PCIS to make a few suggestions our members feel would not only enhance the existing partnership but also improve our country's ability to manage exceptional events.

First, let the partnership mature. It is working, but it's still young. We have accomplished a great deal with DHS since its inception and adoption of the PCIS as the framework for private-sector engagement, and even more in the year since Secretary Chertoff exercised the Section 871 exemption and created CIPAC. We are still exploring ways to use that framework.

We welcome the involvement of Congress, but we need to continue a trusted environment in order to work with our government partners on sensitive issues affecting our safety and security.

We would be happy to work with you as you consider standards and risk assessments so we can build on the trust we have established and capitalize on the free flow of ideas and solutions we are beginning to enjoy under the new framework.

Second, help us educate all Federal departments and agencies regarding the nature of this partnership. The partnership model is a good one, but not uniformly executed across the sectors. This is due, in part, to the need of some in the Federal government to be educated on the value of the partnership model. Many we work with in DHS' operating group for IT and communications and the Department's Partnership and Outreach Division understand the structure, but the further one gets away from those offices, the less understanding and appreciation of the Sector Partnership Framework there is.

We also need help internationally. The public-private partnership is the right model globally, and as other countries grapple with these same issues, the U.S. government can continue to lead, and even increase, global education efforts touting the benefits of public-private partnerships, and the primacy of ensuring innovation and flexibility in the critical infrastructure discipline.

Third, we must reform the National Response Plan (NRP) process to reflect the true partnership model we have found with the development of the NIPP. Additionally, the NRP text and annexes should be reviewed to include more private-sector participation early in response actions. This is important when dealing with physical incidents, but even more important when you consider the cyber dimension. Critical infrastructure owners and operators understand their interdependencies, especially on the global arena. PCIS considers all cyber incidents international by default. The private sector already has multiple collaborative mechanisms in place to deal with significant cyber incidents. Many Internet Service Providers (ISPs) collaborate through the informal "nsp-sec" community. Multiple government and private-sector incident response teams belong to the more formal Forum of Incident Response and Security Teams (FIRST). These two global organizations respond in real time, and we should begin thinking of them as "global cyber first responders." The NRP should incorporate turning to these organizations, and other private-sector organizations like them, for any cyber incident of national significance.

Fourth and finally, the government must share more timely and useful information with the private sector. It is often difficult to determine exactly who "needs to know" sensitive information, but the Sector Partnership Framework includes enough trust to err on the "need to share" side of the equation. Complex interdependencies, a lack of familiarity with sector operations, and little-known collocation of assets argue for the sharing of alerts and warnings with PCIS and relevant ISACs rather than trying to ferret out only those owners and operators that government analysts think might be involved in an incident. Many of the ISACs are capable of transmitting and storing classified material, and many sectors have cleared individuals that can be trusted with sensitive information. The Emergency Notification System (ENS), for example, has worked well on the few occasions DHS has used it. DHS has done a relatively good job establishing it, though it the Department could exercise it more frequently and should update it regularly with a PCIS list, ISAC list, and other key executives, as required.

Thank you again for the opportunity to be with you today on behalf of PCIS. Now I would be happy to answer any questions you have.