Critical Infrastructure Interdependence: Public-Private Roles and Responsibilities

Testimony of Kenneth C. Watson
President and Chairman
Partnership for Critical Infrastructure Security

Before the
House Select Committee on Homeland Security
Subcommittee on Cybersecurity, Science, and Research and Development
Subcommittee on Infrastructure and Border Security

Hearing on

Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness

September 4, 2003

Chairman Thornberry, Chairman Camp, Congresswoman Lofgren, Congresswoman Sanchez, Congressman Cox, Congressman Turner, and other Distinguished Members: thank you for the opportunity to testify today regarding the interdependence of our critical infrastructures. The nearly universal dependence on privately owned and operated infrastructures, their dependence on computer networks, and their interdependence on each other, were the primary drivers prompting the creation of the President's Commission on Critical Infrastructure Protection (PCCIP, "The Marsh Commission"), which reported its findings in October 1997. We have made a lot of progress in the six years since the Marsh Commission published its report, but there is still much to be done. The attacks of September 11, 2001, the northeast blackout of August 14, 2003, and the rapid sequence of Internet worms seen in the last three weeks highlight the need to maintain a sense of urgency as we continue to address these issues.

My background. I am President and Chairman of the Partnership for Critical Infrastructure Security (PCIS), launched in December 1999 as industry's response to the Federal government's call for public-private partnerships following the publication of the Marsh Commission report and the subsequent issuance of Presidential Decision Directive 63 (PDD-63) in May 1998. I also manage Cisco Systems' involvement in critical infrastructure assurance activities. In 1997 I retired from the US Marine Corps after 23 years of service, the last eight of which were devoted to what is now known as Information Warfare or Information Operations. My last tour of duty in the Marines was as Marine Liaison Officer to the Air Force Information Warfare Center in San Antonio, Texas, where we advanced the art of defending against attacks against information and information systems. The thought processes behind the defensive planning, modeling, and exercises we conducted ten years ago apply directly to the problem of critical infrastructure protection today.

PCIS. Following the Marsh Commission recommendations, in 1998 the Federal government established several organizations and positions to coordinate critical infrastructure protection efforts, and recommended the creation of "sector coordinators" in each critical industry sector to coordinate across each industry and with appropriate Federal lead agencies. Working with industry leaders, lead agencies initially appointed eight individuals, most from industry trade associations, as sector coordinators. Some sectors have more than one coordinator because of their size and complexity.

The PCIS is the forum for cross-sector and public-private dialog on reducing vulnerabilities, mitigating risks, identifying strategic objectives, and sharing sound information security practices. It is a public-private partnership that is also a non-profit organization run by companies and private-sector associations representing each of the critical infrastructure industries. When we created the PCIS, we structured the Board of Directors so that the sector coordinators would always be its majority. The number of Directors is flexible, anticipating the creation of additional sectors and naming of new sector coordinators. There are currently twelve sector coordinators, representing five of the thirteen sectors outlined in the National Strategy for Homeland Security. Ten of

these are on the PCIS board. The current list, including the Federal lead agencies and representatives, is attached. The mission of the PCIS is to coordinate cross-sector initiatives and complement public-private efforts to promote the reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

In the four years since its creation, the PCIS has accomplished a great deal. A PCIS public-policy white paper on barriers to information sharing got the attention of Congressmen Davis and Moran, who co-sponsored the first bill to provide a narrowly written exemption to the Freedom of Information Act (FOIA) for critical infrastructure information. Senators Bennett and Kyl followed with a similar bill, and after conference committee work, the provision is now part of the law that created the Department of Homeland Security (DHS). PCIS also coordinated industry input to the National Strategy to Secure Cyberspace, offering each of the sectors' strategies and an overview document comparing commonalities and differences on the PCIS web site. The PCIS developed an information sharing taxonomy, including the terms commonly used by all industry Information Sharing and Analysis Centers (ISACs) and government agencies that share cyber vulnerability, threat, and solution information. Currently, the PCIS is working on an interdependency risk assessment handbook, and the board, including the sector coordinators, meets monthly by teleconference to discuss cross-sector critical infrastructure protection issues.

Interdependence Examples. We all depend on telecommunications—in fact, when recently asked to list their dependence on other sectors, the sector coordinators rated telecommunications as first or second on their list. Nearly equal to telecommunications was electric power. Without electricity, there is no "e" in e-commerce. However, without railroads to deliver coal, the nation loses 60 percent of the fuel used to generate electricity. Without diesel, the railroads will stop running. Without water, there is no firefighting, drinking water, or cracking towers to refine petroleum. Without financial services, transactions enabling all these commodity services cannot be cleared. Yet, these are not just one-way dependencies. When the railroads stopped running after 9/11 to guard hazardous material, it only took the city of Los Angeles two days to demand chlorine or face the threat of no drinking water—the railroads began operating again on the third day. Throughout the Northeast, dependencies on electric power were obvious. Some areas had electric water pumps, and they had to boil their drinking water for days after the blackout.

Gaps and barriers

Sector Coordinator Roles Poorly Understood. The role of the sector coordinator is not well understood, either in industry or government. DHS is developing a "best practices" guideline for sector coordinators, and working with lead sector agencies and industry leaders to identify organize new sectors from which candidates for the job will emerge. New sectors have been identified by the National Strategy for Homeland Security, but no sector coordinators have been named. In many critical infrastructure industries, CEOs and other executives are not aware of the role of sector coordinator,

do not know who their coordinator is, and use other means to coordinate their critical infrastructure assurance actions. Industry sectors are neither homogeneous nor hierarchical, but in the rapid-paced, complex world of critical infrastructure assurance, single "belly-buttons" are absolutely needed to coordinate actions within and across critical sectors.

Interdependence vulnerability research inadequate, incomplete, and underfunded. All of our critical infrastructures are interlinked in complex, sometimes little-understood ways. Some dependencies are surprising, contributing to unusual key asset lists. Studies, modeling, and exercises represent the three primary interdependence research methods.

Studies. Some rudimentary research has been done on interdependencies, but it has only been sufficient to illuminate how important this type of modeling and analysis could be. Sandia and other national labs have initiated interdependency studies, looking at intersections with the energy sector. The National Security Telecommunications Advisory Committee (NSTAC) has done similar work, addressing intersections between telecommunications and other sectors. The National Infrastructure Advisory Council (NIAC) has a current effort to develop policy recommendations on interdependency risk assessments. The sector coordinators are involved in that study, which will become available after delivery to the President in the October timeframe. The PCIS is coordinating with this NIAC working group to ensure that the handbook we develop is in harmony with NIAC policy recommendations.

In the FY2004 Budget submitted to Congress, approximately $500 million has been requested to assess the security of the nation's critical infrastructure. Of this, $200 million is allocated to develop and maintain a primary mapping database, and $300 million has been allocated to work with states and industry to identify and prioritize protective measures to mitigate any risks identified through the ($200M) database consequence-mapping activity. We expect this level of funding to grow at a rate of about 2% per year over the next five years.

While this seems like a lot of money, there is concern that the complexity associated with this type of analysis is not readily recognized. Conducting cross-sector vulnerability assessments presumes that each of the individual sectors has already been modeled. This is not the case. Each sector will need to be modeled to some degree of fidelity before any cross-sector studies can be accomplished. These individual sector models must incorporate how the network elements work, their capacities, how they connect to each other, and where they connect to each other. It is not sufficient to simply ask the sectors' major infrastructure owners for a list of their key assets and critical nodes, so that they can be "mapped." Mapping an asset without modeling how it works or how it connects to or impacts the next element in the network is an exercise without merit. The network owners already know their key assets and critical nodes—what they don't know is whether their key assets and critical nodes are in the same geographic vicinity as their competitors' nodes, or whether underlying or supporting infrastructure is in fact, truly diverse. In highly competitive sectors, such as

telecommunications or finance, it would not be unusual to find that each of the major providers has intended to buy diversity and redundancy from numerous entities, only to find that all these entities use the same underground conduit for transport that goes through the same underground tunnel, and they are powered by the same power generation plant. The NSTAC has studied the implications of these types of cross-sector dependencies and has developed a number of programs that the telecommunications sector uses to mitigate these risks. It is time, however to take it to the next level, covering all cross-sector and multi-sector interdependencies.

Modeling. Existing computer modeling and simulation has not been effectively utilized for critical infrastructure protection purposes. DoD operates high-fidelity models to support military missions. DoD is not funded for homeland security, and its modeling capability is probably fully utilized for the purposes for which it was designed. However, DHS could take advantage of DoD model designs and algorithms, applying critical infrastructure data and missions. DoE national labs use sophisticated models to help with energy planning, and they have developed the National Infrastructure Simulation and Analysis Center (NISAC), which is now part of DHS. NISAC capability is still being developed by DHS. Modeling can help develop plans, and it can save some of the expense and time required for regional exercises, but (a) the data used must be up-to-date industry data; and (b) sector coordinators (and the infrastructure owners they represent) must be the primary beneficiaries of modeling results—after all, the sector coordinators are responsible for developing and executing plans to protect critical infrastructures. One of the challenges will be that much of the data required may be proprietary..

To date, the NISAC has centered its modeling efforts on the energy sector. To understand the complexity of this modeling problem, consider the NISAC model of the energy sector as a baseline, and apply it as a level of magnitude to the telecommunications sector. While we do not know the precise amounts, it is our understanding that the current electrical sector modeling cost about $30-40 million to develop and was done over the course of 3 to 8 years. If you assume that the level of detail developed within the electrical sector model is appropriate (and we do not know that to be the case) and simply multiply this $30-40 million times the number of facilities-based networks that comprise the telecommunications sector, then you would conservatively multiply this estimate by a factor of 9 networks (5 wireless + 1 wireline + 2 IXC + 1 paging), resulting in a baseline model for telecommunications in the $270-$360 million range. Even if all $200 million was dedicated to telecommunications modeling, it would take 1 to 2 years of currently allocated funding, and an even longer actual modeling effort, to model telecommunications alone. Multiply that by 12 sectors, and then you can start on the cross-sector interdependency modeling.

The sectors, particularly the telecommunications sector coordinators, have initiated conversations with the national labs to determine how this important work could be undertaken, and what level of support the national labs would need to marry their modeling, testing and data mining expertise with industry knowledge regarding how the various networks work and how they interrelate to each other within the sector. This

project will require government funding, and the sectors are prepared to work with DHS to develop the most appropriate approach for each sector. It is our sense that various capabilities from numerous national labs (DoE, DoD, etc) will be needed to develop a model that can be built once, routinely refreshed by industry and used by many, in the analysis of vulnerabilities and the development of mitigating strategies. It is also our sense that in the absence of higher funding levels, this statutory requirement may take a decade to accomplish and any benefits to the sectors watered down significantly. This information has not been communicated fully to DHS—the department is still undermanned in this area. This is not an accusation or complaint, but simply a reflection of start-up reality. The sectors are prepared to work closely with DHS once it is ready.

Exercises. DHS has begun to sponsor regional exercises to identify vulnerabilities, dependencies, and cross-sector points of contact for the purpose of developing contingency plans to respond to physical and/or cyber attacks. This effort must be accelerated and expanded to cover every region of the country. Lessons learned must be shared with the sector coordinators so that all the critical industries on the front lines of defense can understand what they need to do and with whom to coordinate.

"Top-off" and "Top-off 2" represented small steps toward addressing physical threats, but these were exercises with little private-sector input or expertise, and certainly no funding for the insertion of this expertise into these exercises. "Livewire" is an upcoming cyber exercise that will have some private-sector input. Feedback from the sectors to date is that these small-scale exercises serve primarily to educate government consultants and do not benefit critical infrastructure owners and operators, who have the responsibility of acting first during a crisis. Regional exercises are a must for the physical dimension, and sometimes cyber exercises will be national in scope. To be effective, they must include private-sector experts to help build the exercises, design scenarios, and participate as key stakeholders. Funding must support private-sector participants' time as it currently does that of the government consultants. More importantly, their design should encourage private sector involvement by telling them things they need to know (e.g., business continuity planning). These exercises must include both the cyber and physical dimensions of critical infrastructure planning, and must involve all the critical infrastructure sectors to ensure a complete understanding of interdependency. The PCIS and the sector coordinators would be happy to work with DHS and other government stakeholders to plan and execute such a series of interdependency exercises.

Recommendations for DHS

Coordinate with lead agencies and industry leaders to rapidly organize the newly named sectors, identify appropriate sector coordinators, and clarify sector coordinator roles. Actively promote the sector coordinator function to key industry and government executives, and within the federal government.

Coordinate with all appropriate national labs and Federal departments working to apply appropriate computer models and simulations to critical infrastructure mission areas. Ensure that sector coordinators and their constituents are involved in establishing modeling objectives and peer review of model creation, data mining, and results. Assure the protection of sensitive data.

Sponsor a comprehensive set of regional and national exercises that cover the physical and cyber aspects of attacks on critical infrastructures, as well as dependencies. Assure the protection of sensitive data, and ensure that sector coordinators and their constituents are involved in exercise design, scenario creation, participation, and are the primary recipients of exercise lessons learned and other information they need to defend their part of the critical infrastructures.

Conclusion. DHS leadership has been very inclusive of industry as they organize to protect critical infrastructures. Everyone in government must understand that in this area, public-private partnership is not just for appearances—it is absolutely essential. Since critical infrastructure owners and operators are on the front lines, the sector coordinators must be part of all critical infrastructure planning, strategy development, exercises, remediation, and responses to threats and attacks. DHS cannot be expected to protect critical infrastructures alone—industry must become part of its organizational culture as it matures. National and economic security are forever intertwined. The industry leaders I work with understand and embrace their role as front-line defenders, and are willing to do their part to protect our national and economic security.