TESTIMONY

CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE?

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

To
US Senate
Committee on Governmental Affairs

October 4, 2001

Good morning Chairman Lieberman, Senator Thompson, and distinguished Committee Members. I am honored to be here today on behalf of the more than 70 companies and organizations that comprise the Partnership for Critical Infrastructure Security, or PCIS. The question you are asking, "Critical infrastructure protection: who's in charge?" appears aimed at discovering leadership. America would like to be able to turn to a single government executive or agency, and perhaps one industry belly button, with the authority and responsibility to assure the continued delivery of vital services to our citizens in the face of new and emerging threats. What you will actually discover is an architecture that requires distributed leadership, cooperation, and *partnership* to accomplish that goal.

The need to coordinate and manage the assurance of our nation's critical infrastructures is not something industry and government just started considering since September 11. The members of the Partnership and our government counterparts have been working on this since 1999, and some industries, such as the telecommunications sector, have had formal working relationships with government agencies dating from the early 1980s. I'd like to describe for you the environment of the critical infrastructures, explain what we were doing before the horrendous attacks three weeks ago, and what has changed since then. I'll also have recommendations for the Congress and the American people.

The Architecture

Over the last 10 to 20 years, the United States, and the rest of the developed world, have truly changed the way we live and work, and there is no turning the clock back. Each industry is now dependent on every other, and we are all dependent on computer networks. The Federal Government cannot function without services provided by private-sector infrastructure owners and operators. Many of these are multinational corporations, and all have an interlaced network of suppliers, partners, and customers. The Internet itself relies on key nameservers and routers located around the world, with no central ownership or authority. The health of the global economy is directly relevant to the health of America's national and economic security.

Just as the Internet is open, borderless, international, and unregulated, responsibility for protecting critical infrastructures is distributed among companies and government organizations. Distribution of control is actually safer than centralization, and builds resilience into the architecture. Form follows function. This applies not only to architecture, but also to how we organize to protect our critical infrastructures.

Even with the best of intentions and the most modern tools, the Defense Department could not defend America against a cyber attack on a power plant in Omaha, that happens to provide power to a major railroad hub's switching center. Critical infrastructure protection requires a true public-private partnership, with all the trust that implies, to succeed. Activities that an enterprise can take—conducting vulnerability and risk assessments, deploying security technologies, investing in research and development, creating incident response teams— must now be distributed and coordinated. Many in industry and government have been focusing on exactly how to accomplish this coordination for at least the last five years.

Partnerships

The President's National Security Telecommunications Advisory Committee, or NSTAC, was established in 1982 to provide advice on national security and emergency preparedness issues in the telecommunications sector. Comprised of most key service and equipment providers, the NSTAC has consistently discovered and made recommendations to mediate problems in that critical infrastructure.

The President's Commission on Critical Infrastructure Protection, reporting in October 1997, recognized that the need to coordinate closely between the public and private sectors for economic and national security no longer applied to a single infrastructure sector. The Marsh Commission correctly identified the vulnerability of all our infrastructures to errors and intentional attacks, their interdependency in both the cyber and physical dimensions, the dependence of government on private-sector infrastructures, and the resulting requirement for a robust public-private partnership to develop solutions. Industry responded to the government invitation to a dialog by launching the Partnership for Critical Infrastructure Security at the World Trade Center on December 8, 1999.

Since its formation, the PCIS has become a model for cross-sector coordination, public-private cooperation, and a clearinghouse for timely information needed by critical stakeholders. Last year, the PCIS identified barriers to information sharing with government, and now the Congress is working through legislation based on our findings. During the response to the Code Red worm, the PCIS represented industry alongside the FBI and security experts as we made the public service announcement that ultimately blunted the impact of that infestation. Later this year, the government will publish the unique public-private National Plan, with industry sections coordinated by the PCIS.

I mentioned before that this is not just an American problem. Several countries are following our example, establishing similar partnerships. The PCIS is forming close relationships with them, and we plan to collaborate in several key areas. Earlier this year, Canada established the Office of Critical Infrastructure Protection and Emergency Preparedness, and its head, Margaret Purdy, has attended several PCIS meetings. We are using the results of Canada's outstanding interdependency vulnerability study as we look at our own. The United Kingdom recently formed the Infrastructure Assurance Advisory Council, and its Executive

Director, Dr. Andrew Rathmell, will be speaking at the next PCIS Board meeting later this month. Switzerland's Infosurance program is a public-private infrastructure security partnership very similar to ours. In August this year, the United States and Australia held a bilateral meeting in Canberra, where we agreed to collaborate on several key initiatives, including international security standards.

There are several other public-private and international partnerships: the Forum for Incident Response and Security Teams, or FIRST; the Worldwide Information Technology Security Association; and others, mainly in the information technology sector. Many people and organizations are beginning to grasp the significance of the distributed nature of the new economy, its implications on economic and national security, and the absolute requirement for partnership and collaboration.

Information Sharing

One of the keys to success is effective and timely information sharing about threats, vulnerabilities, countermeasures, and best practices within and between industries, and between the public and private sectors. Information Sharing and Analysis Centers, or ISACs, are proving their value as both computer defense centers and awareness vehicles. There are currently five ISACs in operation:
Financial Services
Telecommunications
Information Technology
Electric Power
Oil and Natural Gas

These ISACs have shared information on threats to members and helped their sectors prevent damage and disruption from threats like Code Red, Nimda, and Vote. The Telecom ISAC, with its connections to National Infrastructure Protection Center (NIPC), Joint Task Force –Computer Network Operations (JTF-CNO), FedCIRC, and National Communications Systems (NCS), is able to share vital information from the government to industry that has proved both valuable and timely.

Four additional ISACs are in various stages of development:
Railroads
Aviation
Water
Information Service Providers

One of this year's top goals for the PCIS is to establish a cross-sector and public-private information-sharing architecture. The existing ISACs, under the leadership of the NCS, met on September 26, 2001 to develop operational information-sharing capabilities. This meeting greatly accelerated the progress we have made in this area, and the procedures they develop will form the foundation for the overall PCIS cross-sector architecture. They agreed to the following steps:
ISAC operational elements will immediately exchange e-mail, telephone numbers, and operational interfaces.

ISACs will pass traffic deemed appropriate to other sectors that does not duplicate publicly available information, but addresses concerns to both physical and cyber elements of sector infrastructures.

The Telecom ISAC will draft an SOP in one week (due yesterday), using operating rules from all the ISACs.
The Telecom ISAC will provide a phone bridge that any ISAC can use to initiate an alert to all.
NCS will offer a port to any ISAC operations center wishing to join the ACN
as a second tier of communications.
The ISACS will establish this pilot program for 60-90 days and then assess expanded participation.
NCS provided GETS cards to ISAC operations centers.
The Telecom ISAC will share government information as widely as possible with all ISACs.

What changed on September 11?

Information technology took a huge hit on September 11. In addition to the people that we can never replace, one estimate places losses in IT resources by the financial community alone at $3.2 billion.

Verizon's switching office at 140 West St. in Manhattan, supporting 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites.
AT&T lost fiber optic equipment in the World Trade Center and had switching equipment damaged in a nearby building. Remarkably, AT&T switching gear in the basement of the World Trade Center continued to function.
Sprint PCS wireless network in New York City lost four cells.
Cingular Wireless lost six Manhattan cell sites.
Worldcom lost service on 200 high-speed circuits in the World Trade Center basement

But like the United States, the Internet was created as an open society, with multiple communications paths and built-in resilience. Because of its redundancy, the Internet provided many of the needed paths for communication immediately following the attacks in New York and Washington.

The day of the attack:

AOL Instant Messenger logged 1.2 billion messages – 100 times usual message volumes.
Verizon and AT&T reported that call volume and long-distance traffic doubled

One week after the attack, Verizon announced that it had restored 1.4 million of 3.5 million data circuits, and the New York Stock Exchange had phone and data service to 14,000 of its 15,000 lines. The exchange handled 2.37 billion transactions without incident on its first day back in operation.

Other infrastructures also demonstrated tremendous robustness and cooperation. Diesel generators were brought in to provide power for lighting, telecommunications, and Internet access in lower Manhattan. All the involved sectors and governments worked together, overcame a restriction on diesel fuel deliveries, and accomplished the miracles we have all witnessed.

The terrorist attacks on the World Trade Center and the Pentagon did not change the architecture of the new economy, our interdependency, or the interlinked nature of the economies and national security of the nations of the develop world. What those attacks did was to create a sense of urgency and a need to “do something” about security among those that had paid little attention to security before. Just as the Administration carefully and deliberately seeks out those that conducted and supported these barbaric acts and learns about this new battlefield environment, I urge the Congress, the Administration, and the American people not to move too quickly to try to solve the infrastructure protection problem.

The challenge for this Administration is to streamline its organization to become an effective partner to industry. The current mix of lead agencies, sector liaisons, and uncoordinated budgets makes synchronized action difficult. The Critical Infrastructure Assurance Office (CIAO), working with the National Coordinator for Security, Critical Infrastructure Protection, and Counter-Terrorism, has overcome immense obstacles and achieved a high level of cooperation and coordination among government departments and agencies.

We believe the events of September 11 will also ultimately result in changes to the National Plan for Critical Infrastructure Protection, for which the PCIS plays a key coordination role. We will work closely with the CIAO as the government organizes itself to manage Homeland Security, Counter-Terrorism, and Critical Infrastructure Protection. We are confident that there will be much more on cross-sector reconstitution in the plan than originally envisioned.

Recommendations

So what can we do to protect our critical infrastructures? We can raise the bar of security worldwide, through research and development, interdependency vulnerability studies, information sharing, raising awareness, and removing legislative barriers.

Support Administration initiatives to streamline coordination within the Federal Government. Any overall federal coordinator must have budget authority and accountability to be effective.
Support initiatives that will secure the next-generation network of networks as well as the patches and fixes we are applying today. The PCIS is developing a research and development road map that will include a gap analysis of current industry, academic, and government programs, and recommendations for focusing resources to meet sector and cross-sector needs.
Encourage government organizations, businesses, and individuals to practice sound information security. Several organizations publish lists of effective means to secure computers and networks against malicious activity, like updating passwords, disallowing unauthorized accounts and unneeded services, and installing firewalls and intrusion detection. This is now not just common sense, it is a matter of cyber civil defense.
Carefully consider the impact of any new legislation on the freedoms Americans cherish—individual privacy, freedom of expression, and entrepreneurship. We all understand that without security there is no privacy, but we must always strive for balance.

The PCIS Public Policy Working Group is investigating many areas of current and pending legislation with the purpose of discovering ways to improve critical infrastructure assurance at all levels. We welcome any invitation to discuss our activities with you at any time. We believe a dialog where we can hear your insight, and you can hear our concerns, will be healthy and fruitful.

We are all in this together—industry, academia, the Administration, the Congress, and the American people—and we need all points of view to ensure that our critical infrastructures continue to provide for the health and welfare of all citizens and the pursuit of liberty.

Thank you very much. I'm happy to answer any questions you have.

PCIS Board of Directors

Association of American Railroads	Ed Hamberger, President
Association of Metropolitan Water Agencies	Diane VanDe Hei, Executive Director
Bank of America	Rhonda MacLean, Chief Information Security and Business Continuity Officer
BellSouth Corp.	Bob Wright, Director, Information Security
Cisco Systems, Inc.	Ken Watson, Manager, Critical Infrastructure Assurance Group
Consolidated Edison Company of NY	Lou Rana, Vice-President
Information Technology Association of America	Harris Miller, President
The Institute of Internal Auditors	Bill Bishop, President
Merrill Lynch & Co., Inc.	Steve Katz, Chief Security and Privacy Officer
Microsoft Corporation	Howard Schmidt, Chief Security Officer
Conoco, Inc.	Billy Gillham, Manager, Global Security
North American Electric Reliability Council	Michehl Gent, President
Telecommunications Industry Association	Gerry Rosenblatt, Director, Technical and Regulatory Affairs
Union Pacific Corporation	Rick Holmes, Director, Information Technology
United States Telecom Association	Fred Tompkins, Director, Network Assurance

PCIS Relationships

Committee Members | Subcommittees | Hearings | Key Legislation | Jurisdiction
Press Statements | Current Issues | Video of Select Hearings | Sites of Interest