TESTIMONY

"CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE?" COMMITTEE ON GOVERNMENTAL AFFAIRS

THURSDAY, OCTOBER 4, 2001
9:30 a.m. Room 342
DIRKSEN SENATE OFFICE BUILDING

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, members of the Committee on Governmental Affairs, it is an honor to appear before you today to discuss the Federal government's ongoing efforts to help secure our nation's critical infrastructures. Earlier efforts are described in some detail in the *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001*.

The Committee on Governmental Affairs has shown exceptional leadership on a broad range of national and economic security issues. This is particularly true in regard to Critical Infrastructure Assurance. I am therefore grateful for the opportunity to work closely with you and the Congress to develop ways to advance infrastructure assurance for the private sector, for the federal, state and local governments, and in fact, for all Americans.

As you know, President Bush has declared that securing our critical infrastructures is essential to our economic and national security and will be a priority of his administration. The tragic events of September 11th only underscore the urgency with which we must undertake this vital task as one component of a broader effort to secure the nation's homeland against terrorism.

No viable solutions – especially on a matter of such complexity and scope - can be developed or implemented without the executive and legislative branches working closely together, and in the coordinated, complimentary manner that they are.

As vital as our nation's critical infrastructures are to the American Way of Life, the authority to protect those infrastructures must be a priority; and the resources must match the rhetoric. I am excited by the Common Purpose that has joined the Executive and Legislative branches of our great government in implementing an Agenda for Action.

The work of your committee, along with that of others, will make an important contribution to establishing the consensus and leadership focus needed to safeguard critical government and private sector services against both physical and cyber attacks. As we have so recently seen, the enemy is ruthlessly attacking economic targets – our critical infrastructures – in a misguided effort to bend our wills and undermine our resolve.

WHAT ARE THE COMPONENTS OF THE NATION'S CRITICAL INFRASTRUCTURE?

The United States has long depended on a complex of systems – critical infrastructures – to assure the delivery of vital services. Critical infrastructures comprise of those industries, institutions, and distribution networks and systems that provide a continual flow of the goods and services essential to the nation's defense and economic security and to the health, welfare, and safety of its citizens.

These infrastructures are deemed "critical" because their incapacity or destruction – we are painfully witnessing this now - could have a debilitating regional or national impact. These infrastructures relate to:

Information and communications,

Electric power generation, transmission, and distribution,

Oil and gas production and distribution,

Banking and finance,

Transportation,

Water supply, and

Emergency government services.

Critical infrastructure assurance is concerned with the readiness, reliability, and continuity of infrastructure services so that they are less vulnerable to disruptions, so that any impairment is of short duration and limited in scale, and that services are readily restored when disruptions occur.

To complicate matters further, each of the critical infrastructure sectors is becoming increasingly interdependent and interconnected. Disruptions in one sector are increasingly likely to affect adversely the operations of others. We are witnesses to that phenomenon now. The cascading fallout from the tragic events of September 11th graphically makes the business case for critical infrastructure protection. That the loss of telecommunications services can impede financial service transactions and delivery of electric power is no longer an exercise scenario. There can be no e-commerce without "e" – electricity. There can be no e-commerce without e-communications.

Our society, economy, and government are increasingly linked together into an ever-expanding *national* digital nervous system. Disruptions to that system, however and wherever they arise, can cascade well beyond the vicinity of the initial occurrence and can cause regional and, potentially, national disturbances.

PRIMARY THREATS TO THE CRITICAL INFRASTRUCTURE COMPONENTS

Threats to critical infrastructure fall into two general categories:

Physical attacks against the "real property" components of the

infrastructures; and

Cyber attacks against the information or communications components that control these infrastructures.

Infrastructure owners and operators have always had primary responsibility for protecting their physical assets against unauthorized intruders. Yet these measures, however effective they might otherwise be, were generally not designed to cope with significant military or terrorist threats. Nor -- until recently -- did they have to be. The Defense Department, Justice Department, and other Federal agencies have contributed significantly to the physical protection of the nation's critical infrastructures through the defense of our national airspace and borders against attacks from abroad. Clearly the events of September 11th are going to require both government and industry to work together to deal with the new challenges of terrorism against our homeland.

Securing the nation's critical infrastructures against cyber attacks presents yet another difficult problem. The Federal government cannot post soldiers or police officers at the perimeters of telecommunications facilities or electric power plants to keep out digital attackers. There are no boundaries or borders in cyberspace. The vast majority of the nation's infrastructures are privately owned and operated -- government action alone cannot secure them. Only an unprecedented partnership between private industry and government will work.

Assuring delivery of critical infrastructure services is not a new requirement. Indeed, the need for owners and operators to manage the risks arising from service disruptions has existed for as long as there have been critical infrastructures.

What is new are the operational challenges to assured service delivery arising from an increased dependence on information systems and networks to operate critical infrastructures. This dependence exposes the infrastructures to new vulnerabilities. Individuals and groups seeking to exploit these vulnerabilities range from the recreational hacker to the terrorist to the nation state intent on obtaining strategic advantage.

The cyber tools needed to cause significant disruption to infrastructure operations are readily available. Within the last three years alone there has been a dramatic expansion of accessibility to the tools and techniques that can cause harm to critical infrastructures by electronic means. One does not have to be a "cyber terrorist" or an "information warrior" to obtain and use these new weapons of mass *disruption*. Those who can use these tools and techniques range from the recreational hacker to the terrorist to the nation state intent on obtaining strategic advantage. From the perspective of individual enterprises, the consequences of an attack can be the same, regardless of who the attacker is. Disruptions to the delivery of vital services resulting from attacks on critical infrastructures thus pose an unprecedented risk to national and economic security. What if the recent computer viruses – Code Red and Nimda – had hostile payloads in them and did more than just threaten the stability, reliability and dependability of the Internet?

FEDERAL ENTITIES INVOLVED IN INFRASTRUCTURE PROTECTION

Taking the broad view, it would be accurate to say that each Department and Agency in the Federal government contributes to the objective of

critical infrastructure assurance. The heads of executive departments and agencies are responsible and accountable for providing and maintaining appropriate levels of information systems security, emergency preparedness, continuity of operations, and continuity of government for programs under their control.

Under Presidential Directive 63, the previous administration assigned overall responsibility for policy development and coordination for critical infrastructure assurance to the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council.

PDD-63 established the National Infrastructure Protection Center (NIPC) housed at the FBI. NIPC serves as the nation's threat assessment, warning, and incident response center for cyber attacks, and also facilitates law enforcement investigations of cyber-related crimes.

PDD-63 also established the Critical Infrastructure Assurance Office (known as CIAO) as an interagency office located at the Department of Commerce to support the National Coordinator in carrying out these policy development and coordination functions.

CIAO's responsibilities in developing and coordinating national critical infrastructure policy focus on three key areas:

Promoting national outreach and awareness campaigns both in the private sector and at the state and local government level;

Assisting Federal agency analyses of critical infrastructure dependencies; and

Coordinating the preparation of an integrated national strategy for critical infrastructure assurance.

I want to share with you my views on what must be done and what we have done.

Promote National Awareness

Our first responsibility is to raise national awareness about the problem of critical infrastructure assurance. The primary focus of these efforts has been on the critical infrastructure industries. The target audience has been the corporate boards and chief executive officers who are responsible for setting company policy and allocating company resources. The basic message has been that critical infrastructure assurance is a matter of corporate governance and risk management. Senior management must understand that they are responsible for securing corporate assets -- including information and information systems. Corporate boards must understand that they are accountable, as part of their fiduciary duties, to provide effective oversight of the development and implementation of appropriate infrastructure security policies and best practices.

Prior to September 11th, the challenge of our national awareness effort was to present a compelling business case for corporate action. Government concerns about economic and national security, while important, were not generally viewed as sufficiently providing such a

case. Threats of "cyber terrorism" and "information warfare," while legitimate, were not readily executable in the market – they appeared too remote and irrelevant to a company's bottom-line. That has all now changed.

The threats to critical infrastructure are being translated into business impact that corporate boards and senior management understand. Business impact includes operational survivability, shareholder value, customer relations, and public confidence. Corporate leaders are beginning to understand that the tools capable of disrupting their operations are readily available, and are not the monopoly of nation states. The risks to their companies are serious and immediate and, thus, require prompt attention.

In addition to infrastructure owners and operators, awareness efforts have also targeted other influential stakeholders in the economy. The risk management community -- including the audit and insurance professions -- is particularly effective in raising matters of corporate governance and accountability with boards and senior management. In addition, the investment community is increasingly interested in how information security practices affect shareholder value -- a concern of vital interest to corporate boards and management.

Once the private sector acknowledges the problem of critical infrastructure assurance as one that it must solve through corporate governance and risk management, our role has been to facilitate corporate action.

The government should encourage appropriate information sharing within and among the infrastructure sectors and between the sectors and government. The information shared could include system vulnerabilities, cyber incidents, trend analyses, and best practices. The reason companies should be encouraged to share this kind of information is because by doing so they will obtain a more accurate and complete picture of their operational risks, as well as acquire the techniques and tools for managing those risks.

The Federal government also should encourage the infrastructure sectors to work together on developing contingency plans for coordinating their responses in the event of major service disruptions, whatever the precipitating cause. As the infrastructures become more interdependent, there is a growing risk that restoration efforts undertaken by one sector could adversely affect the operations or restoration efforts of another, potentially contributing to further service disruptions.

In addition, the government should work with industry in identifying potential legal and regulatory obstacles that may unduly impede information sharing or might otherwise interfere with voluntary efforts by the business community to maximize information security efforts. For example, some in industry have argued that voluntary information sharing cannot proceed to a fully mature corporate activity until the reach and impact of laws governing anti-trust and tort liability and the Freedom of Information Act are clarified.

CIAO promotes activities that inform business and technology leaders across industry sectors of the need to manage the risks that accompany the benefits associated with reliance on information systems. CIAO focuses on initiatives that cut across industry sectors and are not the existing responsibility of agencies.

CIAO's outreach activities are reflected in the following major initiatives:

The Partnership for Critical Infrastructure Security; and

Outreach to the business risk management community;

Partnership for Critical Infrastructure Security: As individual Federal agencies formed partnerships with each critical infrastructure sector, there emerged a need for cross-industry dialogue and sharing of experience to improve effectiveness and efficiency of individual sector assurance efforts.

The Partnership for Critical Infrastructure Security was convened in response to that expressed need. This partnership of over 70 companies provides a unique forum for government and private sector owners and operators of critical infrastructures to address issues of mutual interest and concern.

The Partnership also engages other stakeholders in critical infrastructure protection, including the risk management (audit and insurance), investment, and mainstream business communities. The Partnership, which builds upon public-private efforts already underway by the Federal Lead Agencies, is organized by industry for industry, with the U.S. Government acting as a catalyst and a participant.

Major topics being addressed by the Partnership include: approaches to assessing interdependency vulnerabilities; multi-sector information sharing; legislative and public policy issues; research and workforce development; industry participation in preparing the emerging version of the national strategy; and outreach to state and local governments.

Business Risk Management Community: The business risk management community, consisting of auditors, financial security analysts, the insurance community, the legal community, and financial reporting boards serve as unique channels of communication to senior leadership of industry. These groups work with industry in assessing business risks, communicating noteworthy changes to those risks, and supporting the management of such risks.

In that regard, CIAO implemented an awareness and education partnership with a consortium consisting of the Institute of Internal Auditors, the National Association of Corporate Directors, the American Institute of Certified Public Accountants and the Information Security Audit and Control Association. This consortium brought the involvement of a number of noted insurance firms, risk management professionals, legal counsel, corporate board members, audit experts, and Wall Street security analysts.

The consortium held a series of five regional conferences, called "Audit Summits." These meetings were hosted or sponsored by prominent companies, such as J.C. Penney, Home Depot, New York Life Insurance, Oracle Corporation, Arthur Anderson, Deloitte & Touché Tohmatsu, PriceWaterHouseCoopers, and KPMG. The target audiences were directors of corporate boards, chief auditors, and other corporate senior executives. The meetings produced a report that provided guidance for corporate boards on managing information security risks.

Federal Infrastructure Dependencies

The Federal government is responsible for performing certain functions and delivering certain services essential to "providing for the common defense," "promoting the general welfare," and "insuring domestic tranquility."

Such functions and services are vital to advancing our national security, foreign affairs, economic prosperity and security, social health and welfare, and public law and order. Examples from the pages of our nations' newspapers include:

The mobilization of our Reserve Forces –

The protection of the U.S. homeland -

The projection of U.S. forces overseas –

The ability to maintain critical government communications during crises involving national security or a national emergency –

Timely warnings of potential terrorist or cyber-activist attack –

And even something as basic but yet important to a significant segment of the population as the delivery of social security checks.

Increasingly, these services depend ultimately on privately owned and operated infrastructures. To advance this vital Federal interest, the government must take a leading role and satisfy a number of requirements.

Each Federal department and agency must identify:

Its essential functions and services and the critical assets responsible for their performance;

All associated dependencies on assets located in other departments and agencies that are necessary to performance or delivery; and

All associated dependencies on privately owned and operated critical infrastructures that also are essential to performance or delivery of services.

The CIAO's Project Matrix was developed to assist civilian Federal agencies in this process.

To illustrate, I will use the example of the Commerce Department's Tropical Prediction Center (the "TPC") in Miami, Florida, which is responsible for providing timely warnings of hurricanes.

Incapacity or destruction of this essential government service could result in considerable loss of life and property. Indeed, thousands of people died during the Galveston, Texas hurricane of 1900 because there was no advance warning of the hurricane's approach and, thus, no one evacuated the city. In 1992, Hurricane Andrew would have been even more devastating than it was had the TPC not been able to provide timely information about the storm, thereby enabling thousands to evacuate from those areas where the storm's predicted strength threatened to be greatest.

Although the TPC is a critical asset, it does not operate in isolation; it

depends on a variety of other government agency assets, as well as assets owned and operated by private government contractors. These include satellite imaging and analysis centers and radio transmission facilities located in Maryland and Pennsylvania.

Operational disruptions at any one of these facilities could impede the delivery of timely hurricane warnings just as effectively as operational disruptions at the TPC itself.

Furthermore, the TPC depends on specific providers of critical infrastructure services to operate, including Florida Power & Light for electric power, and Bell South & MC 2000 for telecommunications. Disruptions to these services also could impede TPC operations that are necessary to deliver hurricane warnings.

Once such critical assets and associated dependencies are identified, Federal departments and agencies must assess their vulnerability to physical or cyber attack. If they are determined to be vulnerable, departments and agencies must develop and implement plans to manage the risks posed by potential attacks to the performance of essential functions and services.

These plans should seek to deter attacks from happening in the first place, protect critical assets from damage or destruction if attacks occur, mitigate the operational impact of attacks if protective measures fail, restore operations if attacks disrupt services, and reconstitute assets if damaged or destroyed during attacks.

Where performance of essential government functions and services depends on privately owned and operated infrastructures, Federal departments and agencies must work with the owners and operators of these specific infrastructure companies -- on mutually agreed upon terms -- to ensure adequate security measures are established and maintained.

Development of a National Strategy

A common vehicle of communicating overall critical infrastructure policy and strategy is essential. A national strategy developed jointly between government and industry is an effective means for arriving at an agreement about respective roles and responsibilities. The purpose of such a strategy is to present an integrated public-private strategy for government and industry to chart a common course toward achieving the overall goal of national critical infrastructure assurance. CIAO is currently in the process of preparing a national strategy – in coordination with other Federal departments and agencies and the private sector.

The resulting document will serve not only as a guide for action, but also as a vehicle for creating consensus in Congress and with the American people on how to proceed. A national strategy will also help to establish the basis with the Congress and the American public for proposing legislative and public policy reforms where such reforms are needed to advance national policy.

The development of a national strategy should not be viewed as an end in itself. It should be part of a dynamic process in which government and industry continue to modify and refine their efforts at critical infrastructure assurance, adjust to new circumstances, and refine the national strategy as appropriate.

CLOSING REMARKS

Thank you for the opportunity to share my views with you this morning. I look forward to continuing our dialogue.

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