Statement of
John S. Tritak

Director, Critical Infrastructure Assurance Office
U.S. Department of Commerce

BEFORE THE
SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

May 8, 2002

Mr. Chairman, members of the Committee, I would like to thank you for bringing attention to one of the most fundamental challenges to national security and critical infrastructure assurance – information sharing.

The Critical Infrastructure Assurance Office (CIAO) is an interagency entity established in 1998 by Presidential Decision Directive 63 particularly to work with the private sector and other Federal agencies to raise awareness about the importance of critical infrastructure assurance, to develop an integrated national critical infrastructure assurance strategy, and to help articulate the business case for this national commerce issue, which heretofore had been primarily viewed as a national security matter. To help facilitate the ongoing dialogue with the business communities, CIAO is appropriately located in the Department of Commerce, specifically in the Bureau of Industry and Security. This successor to the Bureau of Export Administration represents the intersection of national security and business affairs.

To an increasing extent, national security, government's ability to deliver vital services, and business' ability to transact commerce all depend on the critical services supported by U.S. critical infrastructures. Moreover, these infrastructural systems are themselves increasingly interdependent on one another. Accordingly, it has been the policy of the United States to protect critical infrastructure systems against disruption, thereby protecting the public, safeguarding the integrity of economy, and ensuring the uninterrupted delivery of essential human and government services, and the national security of the United States. This policy seeks to ensure that any such disruptions will occur only infrequently, cause the least damage possible, be manageable and of minimal duration. The CIAO plays an integral role in this process.

As this Committee is aware, however, the vast majority of the critical infrastructure facilities in our nation are owned and operated by the private sector. For this reason, the Federal government, acting alone, cannot hope to secure our nation's homeland. Rather, the national policy of infrastructure assurance can only be achieved by a voluntary public-private partnership involving businesses and other private sector organizations and government at the Federal, State, and local levels. Indeed, since 1998, the Federal government has called for an unprecedented partnership between private industry and government to safeguard U.S. infrastructures against the threats of physical and cyber attack – a partnership that embraces the sharing of vulnerability and threat information through a trusted medium and in a trusted environment.

Encouraging the appropriate exchange of information within and among the infrastructure sectors and between the sectors and government provides infrastructure operators with a more accurate and complete picture of their operational risks, as well as the techniques and tools for managing those risks. It is also an invaluable tool to enable the government to direct resources to assist the private sector and to undertake appropriate law enforcement and other activities against wrongdoers.

Towards a Trusted Process

In its simplest terms, national infrastructure security requires trust – our common trust that the critical services upon which our society and economy depend will be robust enough to withstand assault, even deliberate attack, and continue to function as intended. Fortifying trust in our critical systems, however, demands that we first forge genuine trust in our relationship with the private sector partners who bear the front-line responsibility for infrastructure assurance. Establishing this trusted environment – both in fact and in perception – is no small challenge, but it is the task before us today.

Trust in any relationship based on voluntary cooperation requires predictability. Commerce functions best in a predictable and stable economic and political environment. Information sharing, like commerce, requires a predictable and stable process where the outcomes are certain, not when the outcomes are problematic. In other words, the information sharing process operates best when the participants are confident that the information shared will be used for an appropriate purpose and will not be used to harm their business interests.

Both the government and the private sector possess an interest in ensuring the orderly functioning of the national economy. That common interest creates a strong incentive for the private sector to voluntarily take the steps necessary to secure their critical facilities and systems, including sharing appropriate information.

Some in industry have argued that voluntary information sharing cannot proceed to a fully matured corporate

activity until the reach and impact of laws governing information sharing are clarified. What is needed is a process with clear, well-defined rules that bring certainty to the terms of the information exchange. Without a tacit understanding of the rules governing the handling and use of shared information, it will be impossible to build a healthy process for exchange. The absence of such a process places our nation at significant risk.

WHAT INFORMATION IS NEEDED?

National security is fundamentally about protecting the health and safety of the American public; preserving the operational integrity of our free, democratic society, our economy and our government institutions; and safeguarding our way of life. Critical infrastructure assurance, as a subset of the measures that collectively comprise national and homeland security, seeks more narrowly to maintain continuity of the delivery of critical services, and protection of the related facilities, upon which government and our national economy depend to function. In this context, information sharing is not an end in itself, it is merely a means to end, but one that since September 11th has emerged as a central component in the provision of the common defense.

To maximize the capability of all participants to evaluate risks and make more informed investments to augment security measures, the information shared may cover a broad range, depending on the circumstances. Some examples of categories for information sharing include data on system vulnerabilities and interdependencies, threat intelligence and warning alerts, "incident" information concerning various aspects of attacks on or attempts to disrupt infrastructure systems (*e.g.*, the timing of incidents, whether the incident is cyber or physical in nature, the characteristics of the target and the method of attack, etc.); trend analyses, and effective practices. Our security as a nation depends on our collective ability to understand vulnerabilities, detect incidents, prevent attacks, protect essential infrastructures, and, as necessary, rapidly respond and reconstitute systems.

The private sector primarily wants from the government information on potential relevant threats, which the government may want to protect in order not to compromise sources and methods or ongoing investigations. The basic business model is framed around survival: keep the company in business. This imperative requires that the business meet the needs of paying customers while at the same time protecting the interests of shareholders and other investors. These interests, of course, include retaining and increasing the value of the company, increasing revenue and earnings, and maintaining public and customer confidence in the business' operations and management practices, including the oversight of physical and information assets. Implicit in this model is the understanding that operations will be conducted in compliance with applicable laws and regulations.

In contrast, the government needs information from the private sector that will facilitate its ability to (1) monitor and track patterns of attacks; (2) provide warning information to other potentially vulnerable entities; (3) focus outreach and awareness efforts; and (4) undertake effective law enforcement action against perpetrators. Specifically, the government wants detailed information on cyber-network intrusions and system vulnerabilities, which companies may wish to withhold as proprietary. A company may also want to protect the disclosure of certain information to prevent a loss of public confidence in that company's ability to protect its operations and assets. In addition, publication of information about vulnerabilities can also draw additional attacks before protection can be put in place.

Moreover, the amount of information collected by industry and government agencies is potentially overwhelming. Millions of probes are launched everyday on our nation's networks. Some of these represent actual attempts at intrusion. The government can help by being more specific about the characteristics of information it finds most useful to reduce the burden of information sharing on private businesses and help them to manage it. A recent initiative by *CXO Media*, in partnership with the NIPC and the U.S. Secret Service, to streamline reporting forms for voluntary sharing of data by industry reflects the type of private-public partnership that is possible. Unfortunately, even with that result, the same concerns that are the subject of this hearing surfaced in public comment when the product was rolled-out.

We have seen progress, however. Industry sees Information Sharing and Analysis Centers (ISACs) as providing a benefit. Five of the eight critical infrastructure sectors identified in PDD 63 have created ISACs to identify threats and vulnerabilities within their industries and prevent them from escalating and disrupting business operations. Moreover, through the Partnership for Critical Infrastructure Security (PCIS) various industries have engaged in cross-sector dialogues to examine interdependencies, multi-sector information sharing, legislative and public policy issues, research and workforce development, and industry participation in the preparation of the national strategies for homeland and cyberspace security. Collectively, these activities improve the overall effectiveness of sector assurance efforts.

The ISACs have also served to underscore the limits of the private sector's present comfort level for information sharing. For example, for more than five years, industry has repeatedly voiced concern about the possibility that sensitive business proprietary information shared with the government for infrastructure assurance purposes would become vulnerable to public disclosure under the Freedom of Information Act (FOIA). This uncertainty has become a key

impediment to sharing certain information with the Federal government. Similarly, private sector entities have been hesitant to move very far past the formative stages of ISAC development to undertake intensive analysis of vulnerabilities and development of responses due to an expressed concern that such activities might expose them to liability under the antitrust laws.

To the extent that companies perceive that information sharing may, in fact, increase their potential exposure, a common sense risk assessment argues in favor of caution. Addressing the uncertainties concerning potential FOIA and antitrust exposure may not, standing alone, suffice to catalyze all members of the private sector to embrace information sharing. However, it is becoming increasingly evident that some action on these issues by the government is necessary to demonstrate to its private sector partners the importance that the Federal government places on information sharing and on appropriately safeguarding the information that it receives.

Since 1998, the Federal government has been asking private industry to share data about its vulnerabilities but has been unable to resolve the concerns industry has raised about information sharing. Over the course of the last year, several measures have been introduced in both Houses of Congress, which speak to many of these issues. S. 1456, now pending before the Senate, directly addresses industry's concerns relative to FOIA, antitrust, and other potential liability exposure. I believe this bill and others like it represent important attempts to remedy those concerns and to invigorate that trust that I spoke of earlier. I can assure you that they are receiving very serious consideration from the Administration, and I commend it to the attention of the executives of our private sector partners, as well.

Transparency in government and, as the events of September 11th underscored, security of our homeland represent a tension common to our dynamic, capitalistic, open, and democratic system. Harmonizing these countervailing public interests and maintaining the appropriate balance between them is the public policy challenge.

Let me be clear: there are no "silver bullets" here. While legislation such as a narrowly crafted FOIA solution may be needed to facilitate information sharing, standing alone, it is unlikely to be sufficient to achieve that objective. The critical factor is still trust. Equally important is the response of the federal government to information sharing. The government must be a good partner analyzing the data and providing warning and information to the public, infrastructure sectors, or targeted companies.

Another key challenge that will need to be addressed is how the federal government will be able to share information received from the private sector with state and local governments. This presents an equally challenging policy conflict between Federal preemption and states' rights that will require careful and thoughtful consideration and, I believe, coordination and consultation with the Federal government 's State and local government partners.

CONCLUSION

Information sharing is playing, and must continue to play, an important role in advancing our nation' s efforts to secure critical infrastructures in the United States. The American economy is the most successful in the world. However, the same technological capabilities that have enabled us to succeed can now also be turned against us in the information age. Corporate assets and infrastructures can be exploited and turned against the American people, as we witnessed in the events of September 11th. Powerful computing systems can be hijacked and employed to launch attacks that can disrupt operations of critical services that support public safety and daily economic processes. In such an environment, sharing information is essential to both government and industry to make better-informed decisions and to take more timely and effective action.

Thank you for the opportunity to appear before you today. At this time I welcome any questions that you may have.