SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC INFORMATION SHARING"

Testimony Presented to
United States Senate
Committee on Governmental Affairs

by

Harris N. Miller
President
Information Technology Association of America

May 8, 2002

Good morning Mr. Chairman and Members of the Committee. On behalf of the more than 500 member companies of the Information Technology Association of America (http://www.itaa.org), I am honored to appear before you today. ITAA members, representing a broad spectrum of information technology and communications companies, support the very important goal of increasing information sharing 1.) within the private sector and 2.) between industry and government in order to better protect our nation's critical infrastructure and to promote and sustain global physical and economic security.

ITAA and our member companies strongly endorse S. 1456, The Critical Infrastructure Information Security Act and H.R. 2435, the Cyber Security Information Act, and more specifically the current combined language from S. 1456 and H.R. 2435. We call on this Committee and Members of U.S. Congress that have not already indicated their support for this legislation to do so today. For reasons I will outline below, the certainty and trust these bills engender are key to preventing and minimizing future threats to critical infrastructures.

You may have heard the numbers before. According to the 2002 FBI / Computer Security Institute Survey:

- 90% of large corporations and government agencies responding detected computer security breaches within the last twelve months.
- 80% acknowledged financial losses due to computer breaches.
- 44% were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.
- 34% reported the intrusions to law enforcement.

A December 2001 ITAA / Tumbleweed Communications survey found:

- 70% of Americans concerned about Internet and computer security.
- 74% expressed fears that their personal information on the Internet could be stolen or used for malicious purposes.
- 74% said they are concerned that cyber-attacks could target critical infrastructure assets like telephone networks or power plants.

A recent six-month assessment of client activity by Internet security firm Riptech, Inc. found:

- Average attacks per company increased 79% between July and December 2001.
- 39% of attacks appeared to be a deliberate attempt to compromise a specific system or target.

As the U.S. General Accounting Office (GAO) stated in an October 15, 2001 report entitled "Information Sharing: Practices That Can Benefit Critical Infrastructure Protection," information sharing and coordination "are key elements in developing comprehensive and practical approaches to defending against computer-based, or cyber, attacks which could threaten the national welfare."

"…The importance of sharing information and coordinating the response to cyber threats among various stakeholders has increased as our government and our nation have become ever more reliant on interconnected computer systems to support critical operations and infrastructures, such as telecommunications, power distribution, financial services, national defense, and critical government operations. Information on threats and incidents experienced by others can help stakeholders identify trends, better understand the risks they face, and determine what preventative measures should be implemented."[1]

In short, information sharing can:

1) reduce the harm and impact of attacks on critical infrastructures;
2) help the owners and operators of critical infrastructure systems in multiple sectors to determine the nature of an attack;
3) provide timely warnings;
4) provide analysis to both industry and government to prevent future attacks;
5) mitigate attacks in real-time; and
6) assist in re-constitution and recovery efforts.

As I stated at the outset, ITAA supports the very important goal of information sharing. Strong and unwavering support of that goal is why ITAA and its members are cooperating with several other sectors and a variety of government partners in the National Cyber Safety Alliance (http://www.staysafeonline.info), the Partnership for Critical Infrastructure Security (http://www.pcis-forum.org), and the CyberCitizen Partnership (http://www.cybercitizenship.org).

Support of that goal is why ITAA helped found the IT Information Sharing and Analysis Center (http://www.it-isac.org) and is the reason that ITAA has worked to help develop and facilitate private sector input for the Information & Communications Sector into the President's *National Strategy to Secure Cyberspace,* a plan that Presidential Advisor Dick Clarke calls "a living document" that will change as the threats change.

Support of that goal is why ITAA and its sister associations from around the world have prioritized e-security and critical infrastructure assurance as public policy priorities in the 46-country World Information Technology and Services Alliance or WITSA (http://www.witsa.org), and is why ITAA and WITSA sponsored the first Global InfoSec Summit now nearly two years ago.

Support of that goal is why ITAA continues to raise awareness of critical infrastructure assurance and e-security challenges as a business continuity issue, if not a business survivability issue at the CXO and Board level among our member companies and throughout the private sector.

Support of that goal is why ITAA and its members are so committed to building trust-based relationships with law enforcement officials and agencies at every level of government and internationally.

Support of that goal is why ITAA and many of its sister associations -- which represent millions of small and medium business as well as large corporations -- have been in strong support of the *bi-partisan* legislation that I referenced earlier. S. 1456 and H.R. 2435 were introduced in both the U.S. Senate and U.S. House of Representatives last year to remove narrowly defined legal barriers to information sharing within the private sector and between the private sector and government.

Better information sharing is a necessary step to leveling the playing field in the critical infrastructure assurance world. How so? Bad actors have great advantages when it comes to pooling what they know about hacking tools, malicious code, network vulnerabilities and the like. One of the ironies of the Internet is that it can serve as a school for scoundrels, fostering hacker communities, serving as a classroom for future attacks and helping cyber-psychos communicate their exploits.

Meanwhile, sharing information about corporate information security practices is inherently difficult. Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. Information sharing is a risky proposition with less than clear benefits. No company wants information to surface that

[1] Report to Senator Robert F. Bennett, Ranking Minority Member, Joint Economic Committee, Congress of the United States by the U.S. General Accounting Office, October 15, 2001, page 1.

they have given in confidence that may jeopardize their market position, strategies, customer base, investor confidence or capital investments.

Government agencies seek detailed data about computer attacks for the purposes of better law enforcement, earlier detection, and the promotion of best practices in government and industry. Today, however, corporate counsels advise their clients not to share voluntarily the details of computer attacks with government agencies because the risk that such data could ultimately be divulged through the Freedom of Information Act (FOIA) – even over the agency's objections – is unacceptably high.

The bottom line? Uncertainty about whether existing law may expose companies and industries that voluntarily share sensitive information with the federal government to unintended and potentially harmful consequences. This uncertainty has a chilling effect on the growth of all information sharing organizations and the quality and quantity of information that they are able to gather and share with the federal government. We are not talking about a Harvard moot court debate. If we want to improve the way corporate America responds to the threat of critical infrastructure attacks, government needs to give CEOs and their corporate counsels the certainty that this legislation would provide.

Attached to my testimony is a list of several reasons why current FOIA language is not sufficient to protect critical infrastructure information from disclosure. Ambiguity and discretion remain the order of the day when it comes to agency decisions about disclosure of any kind of business confidential data, despite its importance and despite good precedents in some of the Federal Courts. The lack of certainty is of course acceptable in the ordinary course of business; it simply reflects the bias of FOIA in favor of disclosure, a bias with which we do not quarrel. However, critical infrastructure assurance cannot be considered business as usual.

So the bad guys are playing the "run and gun" offense; the good guys are strictly three years and a cloud of dust. Enacting the information sharing legislation before Congress today would eliminate the hacking community's one-sided advantage. With the appropriate protections in place, legitimate businesses and law enforcement agencies can share the information needed to ward off attacks and track down attackers.

I would like to report on steps industry has already taken to promote information sharing and how this process can be improved; I would also like to emphasize two points about the proposed legislation:

1. Government partners have come to the private sector to ask for information concerning current and potential vulnerabilities in various sectors of our national critical infrastructure. The private sector wants consistently to provide comprehensive and detailed information to government on a voluntary basis, but in order to do so have asked that that information be protected.

2. The private sector AND the Federal Government both have agreed for years that it is important to develop and strengthen information sharing processes and organizations within the private sector since we own and operate the majority of systems that make up and protect our country's critical infrastructure. That is why the IT industry -- as well as other sectors -- have formed information sharing and analysis centers.

For instance, the IT industry has adopted a formal approach to the information sharing challenge. In January 2001, nineteen of the nation's leading high tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues. The objective of the IT-ISAC is to enhance the availability, confidentiality, and integrity of networked information systems. The organization is a not-for-profit corporation that allows the information technology industry to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures.

On the telecommunications side of the I&C Sector, an ISAC has been formed by the National Coordinating Center for Telecommunications-Information Sharing and Analysis Center (NCC). Building on the Center for Telecommunications' traditional role as the operational focal point for the coordination, restoration, and reconstitution of NS/EP Telecommunications and facilities, the NCC-ISAC facilitates voluntary collaboration and information sharing among government and industry participants. The NCC-ISAC gathers information about network vulnerabilities, threats, intrusions, and anomalies from various sources, including the telecommunications industry and the U.S. government. That information is then analyzed with the goal of averting or mitigating the effects of computer intrusions on the telecommunications infrastructure. Resulting reports and analyses are sanitized to remove proprietary and classified information and disseminated in accordance with sharing agreements established by the NCC-ISAC participants.

The value of the ISAC approach is found in the ability to acquire and share information with the group in a way that individual group members cannot accomplish. This process often involves the rapid assessment and conversion of information that individual ISAC members had held as proprietary and confidential into a form that can be shared both with ISAC members and with other affected or interested parties. ISACs are exchanging some "sanitized" information between sectors and at times, on a very limited basis, with the National Infrastructure Protection Center or NIPC. The ISAC information product commonly deals with the provision of early warnings of impending attacks, and the establishment of trends in types and severity of attacks. If more legal protections were in place, there could be more sharing of Internet threat and solution information among the ISAC membership and other appropriate organizations, including the Federal Government. ISACs operate successfully because they are a closed community, founded on mutual trust, and focused on prevention before a large attack occurs. They differ markedly from other open communities whose duties are to alert the more general networked public after a breach has occurred.

As the world economy continues to become more international in nature, ISACs will provide a rich source of useful, validated security threat information, for those enterprises that do not, or are not able to, participate in the information security structure. It is by sharing security data that the nation and the world will be able to respond effectively to the continuing and growing threat, both internally and externally, against critical infrastructures.

Two additional points need to be made: First, this entire process is just getting underway. While there are a few examples of the most competitive companies sharing information within a few ISACs, more time is needed before we will be able to measure real success. Relationships of trust and confidence need to be built. That is why the government, through legislation, has a critical role to play NOW, in the formation of the process, and its encouragement.

Second, many in the business community believe that their efforts are hampered by the government's apparent desire for a limited, one-way form of information sharing. Private sector actors are starting to share with government; not enough government information is being shared with the private sector. The government seems to conduct much of its internal conversations about critical infrastructure on the basis of classified information – the kind that can never be shared – and yet it expects the business community to share its own sensitive information without any ironclad assurances of confidentiality, certainly nothing like the treatment accorded classified information. We are not seeking that level of protection, but as we encourage greater sharing we must likewise promote the notion that the communication must flow in both directions.

A lack of certainty is also a decided impediment to sharing critical infrastructure information with government. That kind of information is not "ordinary" and should be entitled to the extraordinary treatment of a complete ban on FOIA disclosure. Legislative proposals address this defect by taking the subject information out of the realm of agency discretion to disclose. We need to close the gate firmly when this information is shared with government.

In addition, there is some question that when information in the possession of one business is shared with another – exactly the process that should be taking place in the world of critical infrastructure assurance information sharing – that fact alone may be enough to deny a FOIA exemption. Many agencies require a submitter of information to demonstrate the steps it has taken to keep information confidential if it expects confidential treatment by the government. It is ironic indeed that evidence of sharing for purposes of protecting cyber security or recovering from an accident or attack could make it LESS likely for government to protect the information from disclosure. Again, we need to close the gate, as would be accomplished by the proposed legislation.

Antitrust concerns are another important potential legal hurdle to information sharing. The antitrust laws focus on sharing information concerning commercial activities. Information Sharing and Analysis Centers (ISACs) should be in compliance with the antitrust laws because they are neither intended to restrain trade nor have the effect of restraining it by restricting output, increasing prices, or otherwise inhibiting competition, on which the antitrust laws generally focus.

We understand that the Department of Justice has offered assurances that business review letters would be forthcoming for information sharing and analysis centers (ISACs) constituted under the Administration's policies. Yet the issuance of even a set of such letters would prove inadequate, for at least three reasons. First, such ISACs would have to be constituted with a view toward satisfying the Department, as opposed to maximally fulfilling their primary mission. Second, there is the unavoidable negative implication for numerous other affected parties not in possession of a business review letter. Third, the ISACs are not the only organizations that have been constituted to share cyber threat information among industry sector members or with Federal agencies.

Again, I have attached a list of several reasons that the Business Review Letter (BRL) procedure does not offer a complete solution to the problem. I would like to highlight two of those points here. First, BRLs will not be issued for hypothetical situations. Only when all the participants are known, the course of conduct is set and the objectives are understood can the DoJ issue a BRL. This will not always – perhaps even not often – be the case with critical infrastructure information sharing, even with the more complete implementation of ISACs, which has not yet taken place. This is an inherent shortcoming in the BRL procedure, and one that can be fixed with a limited antitrust exemption.

Second, to get a BRL, the requestor must be prepared to put considerable information on the public record and make it available for public comment. This leaves information sharing activities subject to vulnerabilities that they should not have to face. In short, while BRLs can help, they do not provide enough of a solution.

Beyond federal FOIA and antitrust, the proposed legislation goes on to clarify that critical infrastructure threat data shared voluntarily with the government would not be disclosed either under the Federal Advisory Committee Act (FACA) or under state FOIA laws. We do recognize the federalism question that the second provision raises. At the same time, homeland defense is creating a need for federal, state, and local bodies to work jointly to a previously unprecedented degree. In some instances, first responders will not be from federal agencies. Information sharing ought not to dead-end at the federal level but should flow all the way down to the first responders. Without the same protection at the state level as at the federal, state agencies will face the same lack of revealing detail that federal agencies are experiencing today.

Finally, the bills also call for limited use protection -- not immunity -- so that critical infrastructure information disclosed to the government cannot subsequently be used against the person submitting the information. Opponents of this legislation state that the provision is a smokescreen for promising unlimited liability to the corporate community. Nothing could be further from the truth. Once again, it bears repeating: the subject of this legislation is information that the government has requested informally from the business community. There is ample reason to grant limited use protection in return for full disclosure of this information intended to help the government accomplish its mission.

There has been, in ITAA's view -- and this view has also been expressed by other associations such as the Edison Electric Institute, the U.S. Chamber of Commerce, the National Association of Manufacturers, the Financial Services Roundtable, Americans for Computer Privacy, and the American Chemistry Council -- a misunderstanding of the legislation by some critics. Again, we are not calling into question the existing FOIA case law, which taken together suggests that a federal agency would win a test case. Rather, we are saying only that the risk of a loss of such a test case – as viewed by the parties bearing the risk – remains unacceptably high. More importantly, corporations should not be required to accept such risks, or the cost of litigation, when reporting significant cyber events in an attempt to protect the public interest. Second, the proposed legislation has only to do with disclosure of computer attack data and critical infrastructure protection. Normal regulatory information gathering will proceed unimpeded, as it should.

In closing, I would like to cite an article from *USA Today* on May 5, 2002: "Government and private computer networks are facing new threats of terrorist attacks, ranging from an attempt to bring havoc to a major city to nationwide disruptions of finances, transportation and utilities. But people with knowledge of national intelligence briefings say little has been done to protect against a cyber attack."

"…Other legislation would make it easier for companies to share information without being subject to antitrust or freedom-of-information laws. Such communication could alert the government to a terrorist attack, as opposed to more common cases of computer hackers targeting a company or agency. It could also help companies defend against attacks."[2]

The threats are out there. Our critical infrastructure is vulnerable. The private sector and public sector must work together to understand, respond to, and prevent these threats. That is why there is clear unity in the private sector in favor of removing disincentives to information sharing and that is why we support legislation in the U.S. Senate and U.S. House of Representatives -- specifically combined language from S. 1456 and H.R. 2435. We call on this Committee and Members of U.S. Congress that have not already indicated their support for this legislation to do so today.

Thank you, Mr. Chairman. I would be pleased to answer any questions that you and/or Members of this Committee may have at this time.

[2] "Cyberspace full of terror targets," by Tom Squitieri, *USA Today*, May 5, 2002.