AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 107–550

SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC INFORMATION SHARING

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MAY 8, 2002

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

80–597 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
ROBERT G. TORRICELLI, New Jersey
MAX CLELAND, Georgia
THOMAS R. CARPER, Delaware
JEAN CARNAHAN, Missouri
MARK DAYTON, Minnesota

FRED THOMPSON, Tennessee
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
GEORGE V. VOINOVICH, Ohio
THAD COCHRAN, Mississippi
ROBERT F. BENNETT, Utah
JIM BUNNING, Kentucky
PETER G. FITZGERALD, Illinois

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
LARRY B. NOVEY, *Counsel*
KIERSTEN TODT COON, *Professional Staff Member*
RICHARD A. HERTLING, *Minority Staff Director*
ELLEN B. BROWN, *Minority Senior Counsel*
ELIZABETH A. VANDERSARL, *Minority Counsel*
MORGAN P. MUCHNICK, *Minority Professional Staff Member*
DARLA D. CASSELL, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Lieberman	1
Senator Thompson	2
Senator Bennett	4
Senator Akaka	7
Senator Carper	19
Prepared statement:	
Senator Bunning	53

WITNESSES

WEDNESDAY, MAY 8, 2002

Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation	8
John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice	10
John S. Tritak, Director, Critical Infrastructure Assurance Office, U.S. Department of Commerce	12
Michehl R. Gent, President and Chief Executive Officer, North American Electric Reliability Council	28
Harris N. Miller, President, Information Technology Association of America	30
Alan Paller, Director of Research, The SANS Institute	32
Ty R. Sagalow, Board Member, Financial Services Information Sharing and Analysis Center (FS ISAC) and Chief Operating Officer, AIG eBusiness Risk Solutions	34
David L. Sobel, General Counsel, Electronic Privacy Information Center	36
Rena I. Steinzor, Academic Fellow, Natural Resources Defense Council and Professor, University of Maryland School of Law	38

ALPHABETICAL LIST OF WITNESSES

Dick, Ronald L.:	
Testimony	8
Prepared statement	54
Gent, Michehl R.:	
Testimony	28
Prepared statement	81
Malcolm, John G.:	
Testimony	10
Prepared statement	64
Miller, Harris N.:	
Testimony	30
Prepared statement with attachments	94
Paller, Alan:	
Testimony	32
Prepared statement	112
Sagalow, Ty R.:	
Testimony	34
Prepared statement with attachments	123
Sobel, David L.:	
Testimony	36
Prepared statement	166
Steinzor, Rena I.:	
Testimony	38
Prepared statement with an attachment	172

Page

Tritak, John S.:
Testimony 12
Prepared statement 77

APPENDIX

Chart with quote from Osama Bin Laden, December 27, 2001, submitted by Senator Bennett 190
Chart entitled "Reporting and Dissemination of Information." Source: The Report of the President's Commission on Critical Infrastructure Protection, October 1997, submitted by Senator Bennett 191
Chart entitled "Coincidence or Attack?" Source: The Report of the President's Commission on Critical Infrastructure Protection, October 1997, submitted by Senator Bennett 192
Chart entitled "Critical Infrastructure Information Security Act" submitted by Senator Bennett 193
Copy of S. 1456 194
Laura W. Murphy, Director, ACLU Washington National Office, and Timothy H. Edgar, ACLU Legislative Counsel, American Civil Liberties Union, prepared statement 214
John P. Connelly, Vice President, Security Team Leader, American Chemistry Council, prepared statement 222
Catherine A. Allen, CEO, BITS, The Technology Group for the Financial Services Roundtable, prepared statement 228

SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC INFORMATION SHARING

WEDNESDAY, MAY 8, 2002

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:33 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Thompson, Bennett, Akaka, and Carper.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good morning.

Today the Governmental Affairs Committee takes up the issue of protecting our critical infrastructure from terrorist attack and the extent to which private industry should share sensitive information both within its own community and with the Federal Government.

This is a matter of longstanding interest to Senator Bennett, who has introduced legislation with Senator Kyl regarding information sharing and our critical infrastructure. I would like to take this opportunity to thank him for his dedication to this matter of critical importance to our national security.

Senator Bennett's legislation, which is called the Critical Infrastructure Information Security Act, would encourage companies to voluntarily share information about critical infrastructure threats and vulnerabilities with the government and among themselves by granting exemptions from the Freedom of Information Act and the antitrust laws.

Senator Thompson and I are working with Senators Bennett and Kyl to evaluate the principles and questions embodied in this bill, which raises important questions about how to better secure our critical infrastructure against what we now must conclude are very real terrorist threats and continuing criminal threats.

Critical infrastructure is a term that I take to cover our financial, transportation, communications networks, our utilities, public health systems, law enforcement, and emergency services. Critical infrastructure has been described as our Nation's skeleton, but it seems to me that it might more aptly be described as our Nation's vital organs. The critical infrastructure is what keeps the country humming. It enables us to interact with one another. It enables us to continue the life of our economy which sustains all of us, and also makes it possible for us to have the highest quality of life on

the planet. The critical infrastructure in that sense is what makes America work.

Many of our critical infrastructures are privately owned, and in this information age are increasingly computer-dependent and interdependent with each other. For several years, the Federal Government has been working to develop a public/private partnership to secure critical infrastructure. Companies are encouraged to share information among themselves about vulnerabilities, threats, intrusions, solutions, and to share information also with the government, which can then, as appropriate, issue warnings and respond accordingly.

Because of our oversight role, the Governmental Affairs Committee has closely participated in these efforts, although Senator Bennett's foresight is such that he was working on this proposal, this bill, before September 11. Our task took on renewed urgency after the events of September 11. We have held a series of hearings in our governmentwide evaluation about how best to protect Americans here at home as well as our infrastructure, and today's hearing builds on that record that this Committee has compiled.

Let me say that if necessary information is not being adequately shared between private entities and the Federal Government, we must address that problem for the safety of all Americans, but we have also got to be concerned, obviously, about unintended consequences, and that would be unduly undermining, for instance, the public's right to know. So there is a balance here to be struck. It is, in that sense, the balance that this Nation has struck since the beginning of its existence between, if I may state it too simplistically, security and liberty. There is a natural tendency now to move along that spectrum towards security after September 11, and it is realistic and responsible to do so, but obviously we do not want to do it in a way that unduly compromises the blessings of liberty which define what it means to be an American and for which we are all grateful, and in that sense which we are fighting to protect in the war against terrorism itself.

So those are the very important and difficult questions that the legislation before us deals with and we will be dealing with this morning.

I look forward to hearing from today's witnesses to learn exactly what kind of private sector information they believe the government needs, to effectively protect the critical infrastructure and the American people; what the experience of industry and government have been regarding information sharing thus far; and, to the extent that there are those who believe that the proposed legislation would be harmful, or reaches too far, why they feel that is so.

Senator Bennett and I certainly agree that the protection of our critical infrastructure is a priority, a national concern now, and I look forward to working with him as we go forward to achieve a good and reasonable solution.

Senator Thompson.

OPENING STATEMENT OF SENATOR THOMPSON

Senator THOMPSON. Thank you, Mr. Chairman.

We certainly are all redoubling our efforts to shore up our defenses after September 11. You point out most of the issues that

we are confronted with. However, there are other issues. The role of the Federal Government, with regard to critical infrastructure, has never been fully defined. We are in need of proposals to define the Federal Government's role, as well as assigning specific responsibilities to the State, local and private sector entities. And while we want to encourage industry to share information with the Federal Government, we are still in need of a framework for dealing with that information, and assurances about what will be done with that information once it is received.

Senators Bennett and Kyl have introduced legislation which is before this Committee, intended to reduce the threat of terrorism by encouraging private industry to share information with each other and with the Federal Government in order to help prevent, detect, warn of and respond to threats.

Originally cast as a cyber terrorism bill, this bill is just as relevant to physical terrorist threats as well. It seems to me that instead of mandating requirements or issuing regulations for the private sector, we should be incentivizing private industry to protect themselves and share information with each other and the Federal Government. At this time I think the Bennett-Kyl bill is on the right track. There are issues and concerns the bill raises, but those are the things we will begin to try to work through today.

One thing is certain, information is vital to this Nation. On September 11, despite great physical damage sustained, information continued to flow across the country. We learned that, for example, Verizon's switching office at 140 West Street in Manhattan, which supported 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites. WorldCom lost service on 200 high-speed circuits in the World Trade Center basement. Spring PCS Wireless Network in New York City lost four cells. Notwithstanding these losses, the telecom infrastructure continued to bring the Nation sound and images of the events, summoned emergency vehicles and alerted the military. But the wireless disruptions we experienced here in DC, which were also experienced in New York, were localized and due to overload. Within 1 week after September 11, Verizon restored 1.4 million of the 3.5 million circuits it lost. The New York Stock Exchange had phone and data service to over 93 percent of its 15,000 lines when it reopened. Information is vital.

The *LA Times* recently reported that a new CIA report makes clear that U.S. intelligence analysts have become increasingly concerned that authorities in Beijing are actively planning to damage and disrupt U.S. computer systems through the use of Internet hacking and computer viruses. This was in the *L.A. Times* April 25.

I do not know why this is a surprise to anyone. In 1998 the Director of Central Intelligence testified in open session before the Committee that several countries, including Russia and China, have government-sponsored information warfare programs with both offensive and defensive applications. So the stakes are very high.

I look forward to hearing from our witnesses today about how we can better protect our Nation's critical infrastructure and its citizens. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Thompson. Senator Bennett.

OPENING STATEMENT OF SENATOR BENNETT

Senator BENNETT. Thank you very much, Mr. Chairman. I appreciate your courtesy and leadership in holding the hearing. We have been talking about this for sometime, and I appreciate your willingness to raise it to this level.

I would ask that the record be kept open for a week to allow interested parties to submit statements and comments.

Chairman LIEBERMAN. Without objection, it will be done.

Senator BENNETT. If I may, Mr. Chairman, I would like to take a little time to just set the scene, as I see it. And I will start out with a chart that shows an interesting quote that came on December 27, 2001.[1] And the quote is being put up there, but you and Senator Thompson and Senator Akaka have a copy of it. Osama bin Laden says, "It is very important to concentrate on hitting the U.S. economy through all possible means . . . look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck. . . ." Making it very clear that he is not just talking about bombing buildings or symbols. He wants to go after the economy. And, obviously, critical infrastructure represents by definition those parts of the economy that he would attack.

I am not quite sure of the number. I have used 85 percent. Some witnesses say 90 percent of the critical infrastructure in this country is owned by the private sector, so that this represents a vulnerability different than any we have ever faced in warfare before. Always before an enemy would concentrate on military targets or production targets that were tied to the military. In this case, as Osama bin Laden's quote indicates, they are going to go after any aspect of the economy that would shut us down. So let us use the more conservative number and say 85 percent of the future battlefield is in private, not public hands. So if the private sector and the government are both targets, they should be talking to each other, and they should be talking to each other in ways that make the most sense.

Now, this is not a new issue. If I can go back to a pair of charts that were prepared 5 years ago during the Clinton Administration by the report of the President's Commission on Critical Infrastructure Protection. The first one[2] has to do with this whole question of reporting and disseminating information, and the President's Commission, under President Clinton, produced this pyramid. And it is a little hard to read, so let me walk you through it, Mr. Chairman.

At the very top of the pyramid are the publicized system failures or successful attacks. We would think of this in terms of the Nimda attack or the "I Love You" virus or other things that have caused economic damage, and the reporting and dissemination of information about things at the top of the pyramid, if you can follow the arrow on the side, is moderate. That is there is a fairly sufficient amount of information. I cannot resist commenting something I

[1] Chart with quote from Osama Bin Laden appears in the Appendix on page 190.

[2] Chart entitled "Reporting and Dissemination of Information" appears in the Appendix on page 191.

was taught many years ago when it came to chart making, which is "black on blue you never do." [Laughter.]

And someone did not notice that when they drew that black arrow.

Anyway, below that top point of the pyramid, there are threats to critical infrastructure that are less well known and less well reported, and beneath those there are system degradations, information about vulnerabilities that are even less well known and less discussed. And then below that where you talk about the vulnerabilities of particular systems, comes the question of interdependencies where one system may be in very good shape but threatened because it is tied to another that is not in good shape, and then finally, the area that is in the very lowest area of reporting and dissemination are those other sources of useful information that would apply to this.

As I was saying, this chart was drawn up during the Clinton Administration and is now 5 years old. Neither we in the Congress nor the administration have done anything formally about this. There has been a great deal of effort put forward during the Clinton Administration being carried on almost frantically in the Bush Administration. But we in the Congress have not responded in any way to try to make the reporting and dissemination of information more widespread. We are still somewhat contented to concentrate entirely on the tip of the pyramid and not look at the things below that.

Now, one of the reasons for the legislation that I have introduced along with Senator Kyl, and we have now picked up some other cosponsors, is to encourage sharing of information voluntarily across the entire spectrum, that is the 85 percent that is in private hands as well as the 15 percent that is in government hands. And, yes, we do want to protect that information from a FOIA request, Freedom of Information Act. The Freedom of Information Act itself allows this to be done. That is there are provisions in the act that say that information need not be shared. But the real focus of the legislation we have introduced is simply to sharpen the definitions of the areas that are already in the act. We are not trying to repeal the act or in any way damage or change its major thrust. We simply want to make the definitions that it already contains a little clearer with respect to this threat.

Now, why would we want to protect information from a FOIA request? Because if we do not, we will not get it. There are private companies who simply will not give us the information if they think it is subject to a FOIA request, perhaps because they want to protect it from competitors. It is voluntarily given. Why should they voluntarily tell their competitors that they are under threat?

Second, they do not want it to be a road map for terrorists. Many people do not realize that you do not have to be a U.S. citizen to submit a FOIA request. Osama bin Laden could find some third party willing to front for him who would submit a FOIA request, find out how successful he was being in one of his attacks, and the FOIA request therefore could become a road map for the terrorists as they seek to be effective in their attacks. Also, we want consistency from agency to agency and we believe that this legislation will allow that to happen.

There is another reason why this information should come to the government, because the government needs to analyze it to determine whether or not the attacks that are coming are real attacks or simply coincidence. Once again, a chart[1] that comes out of the Clinton Administration that is 5 years old, simply raises the question of whether or not a variety of attacks are a pattern coming from a common source or simply coincidence. Here on this map are a series of things that could happen in the Northwest—9–1–1 suddenly becomes unavailable. In my area of the country there is a threat to the water supply. In the Midwest there are bomb threats at two buildings. Some bridges go down. And FBI phones get jammed. An oil refinery has a fire. These things happen simultaneously. Is there a pattern that would indicate that they are being caused by some enemy, or is simply coincidence that they are all happening on the same day? Without information sharing the government analysts who are looking for the possibility of attack simply will not know. They will have to guess. And guessing is never a very productive kind of thing when you are vulnerable.

So again this is a chart that is 5 years old, drawn up during the Clinton Administration to say we need information sharing so that we can determine whether or not this is a coincidence or an attack.

Now, finally if I could put up a chart that I have produced that summarizes the position that we are taking with respect to this bill.[2] We believe that there needs to be information sharing on the circle on the left of the chart. Within private industry people ought to be able to talk to each other. The telephone company that is under some kind of cyber attack ought to be able to check with somebody in the banking industry to see if they are experiencing similar sorts of problems.

Senator Dodd and I introduced legislation with respect to the Y2K on exactly this point. And it was passed, and if I may say so, the world did not come to an end. There was not a shutdown of civil liberties or freedom of information. It was simply an opportunity for two industries that are seemingly different, but that have the same kinds of computer problems, to talk to each other. So we have that circle on the left side where people in private industry can talk to each other to say, "Gee, my facility is under this kind of cyber pressure. Is anything happening in yours that I might know about?" Then comes the arrow at the bottom of the chart where that information is shared voluntarily with the U.S. Government. Perhaps the most important arrow is the one at the top of the chart where the U.S. Government shares back with industry their analysis. Harking back to the earlier chart, they can say, "No, we see no pattern here. If you have a problem, it is probably caused by a disgruntled employee or a private hacker that decided you are a target. There is no indication here of a major attack." Or the information comes back, "Hey, we have analyzed this. What is happening to you in the banking industry is similar enough to what is happening in power or other utilities, that we think this is a concerted effort being mounted by somebody who wishes the entire economy ill." It is that kind of information shar-

[1] Chart entitled "Coincidence or Attack?" appears in the Appendix on page 192.

[2] Chart entitled "Critical Infrastructure Information Security Act" appears in the Appendix on page 193.

ing and analysis sharing that we think will make the entire Nation safer.

So, Mr. Chairman, I appreciate your willingness to hold the hearing. I appreciate your indulgence in allowing me to go on a little longer than is normal for an opening statement to outline where we are. What I hope we can accomplish in this hearing is to determine the degree to which information sharing is needed, how the government can get the information that it needs from the private sector, how the private sector can get analysis and information that it needs from the government, and if there are additional barriers to the sharing of information that we have not addressed in this legislation that could cause us to make changes in it.

With that, Mr. Chairman, I will participate, obviously, in the questioning of the panel, and again, thank you for the leadership you have shown in pursuing this issue.

Chairman LIEBERMAN. Thank you, Senator Bennett. Thanks for a thoughtful statement, and incidentally, by Senate standards, it was very brief. [Laughter.]

Senator Akaka, do you have an opening statement?

OPENING STATEMENT BY SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman for holding this hearing today on information sharing between the private sector and the Federal Government as a part of our national strategy to protect our critical infrastructure.

Such cooperation should be encouraged in order to safeguard America's computer systems from devastating cyber attacks, and I have listened with interest through the Senator's presentation with the charts that shows it so well.

The interdependency and inter-connectivity of government and industry computer networks increase the risks associated with cyber terrorism and cyber crimes. Any security weakness has the potential of being exploited through the Internet to gain unauthorized access to one or more of the connected systems. Information sharing can help protect our national security and critical infrastructure. The necessary exchange of information is furthered through President Clinton's presidential decision, Directive 683, which established ISACs, Information Sharing and Analysis Centers, to facilitate information sharing among private entities. The Directive fosters voluntary information sharing by various entities with the Federal Government to submit sensitive information that is normally not shared to enhance the prevention and detection of attacks on critical infrastructures.

I believe the confidential sharing of information on vulnerabilities to the Nation's critical infrastructures is necessary. However, we must carefully examine legislation like S. 1456, which would make voluntary shared information about critical infrastructure security exempt from release under the Freedom of Information Act. Exempting this information from disclosure might mean that State and local governments would not have adequate access to information relating to environmental and public health laws like the Clean Air Act. We must not provide inadvertent safe harbors for those who violate Federal health and safety statutes. I have heard from a number of my constituents who believe that

measures to ease information sharing through a FOIA exemption would bar the Federal Government from disclosing information regarding toxic spills, fires, explosions, and other accidents without obtaining written consent from the company that had the accident. States and localities are concerned that other proposals would provide companies with immunity from the civil consequences of violating, among other things, the Nation's environmental, consumer protection and health safety laws. We must be careful not to harm the environment inadvertently or bar communities from acquiring vital public health information by enacting overly broad legislation.

I look forward, Mr. Chairman, to hearing from our witnesses on how to promote information sharing between the Federal Government and private sector in a manner that does not turn back existing laws and regulations that protect the environment or public health. Thank you very much, Mr. Chairman, for holding this hearing.

Chairman LIEBERMAN. Thank you, Senator Akaka.

We will now go to the first panel which consists of representatives of the Executive Branch, the administration. Ronald Dick, who is Director of the National Infrastructure Protection Center at the FBI; John Malcolm, Deputy Assistant Attorney General in the Criminal Division of the Department of Justice; and John Tritak, Director of the Critical Infrastructure Assurance Office at the Department of Commerce. We welcome the three of you.

There is a light system here. We ask you to try to keep your opening statements to 5 minutes. With 1 minute left it will go yellow. When it hits red, we are not going to physically remove you, but try to bring it to a conclusion.

I would like to say for the record that the written statements that you have submitted to the Committee will be printed in full in our record. So we thank you for being here, for this very important discussion.

And, Mr. Dick, why do you not begin?

TESTIMONY OF RONALD L. DICK,[1] DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Mr. DICK. Good morning Senator Lieberman, Senator Thompson, and other Members of the Committee. Thank you for the opportunity to discuss our government's important and continuing challenges with respect to critical infrastructure protection.

In your invitation to appear before this Committee, you asked me to address issues related to information sharing and critical infrastructure protection. Because the NIPC is located within the FBI, we have access to a great deal of information from intelligence sources as well as from criminal investigations.

Only a week ago, our 24 by 7 NIPC watch began receiving calls from several of our private sector partners about the Klez.h worm. The worm had spread quickly and had the potential to affect a number of vulnerable systems by destroying critical operating system files. After consulting with our private sector partners and within a few hours of the official notification, we released an alert

[1] The prepared statement of Mr. Dick appears in the Appendix on page 54.

which was immediately disseminated via E-mail and teletype to a host of government, civilian and international agencies. The alert was also posted to the NIPC website. This is only the most recent example of two-way information sharing and how the private sector works with the NIPC.

The NIPC's InfraGard is an initiative to promote trust and information sharing. We have developed InfraGard into the largest government-private sector joint partnership for infrastructure protection probably in the world. More than half of our 4,100 members have joined since I testified before this Committee 7 months ago. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and other critical infrastructure vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of the FBI field offices.

I have created a new unit within the center, whose mission includes building trusting relationships with the ISACs that had been mentioned earlier that represent critical infrastructures. We now have information sharing agreements with seven ISACs, including those representing energy, telecommunications, information technology, air transportation, water supply, food, and chemical sectors. Several more agreements are in the final stages. To better share information, NIPC officials have met with business, government and community leaders across the United States and around the world to build the trust required for information sharing. Most have been receptive to information sharing and the value of the information received from NIPC.

However, many have expressed reservations due to lack of understanding or perhaps confidence in the strength of the exceptions found in the Freedom of Information Act. In addition, concerns about whether the Justice Department would pursue prosecutions at the expense of private sector business interests, and finally, simply reluctance to disclose proprietary information to any entity beyond their own control or beyond the direct control of NIPC.

The annual Computer Security Institute/FBI Computer Crime and Security survey, which was released in April of this year, indicated that 90 percent of the respondents detected computer security breaches in the last 12 months. Only 34 percent reported the intrusions to law enforcement. On the positive side, that 34 percent is more than double the 16 percent that reported intrusions in 1996. The two primary reasons for not making a report were negative publicity and the recognition that competitors would or could use the information against them if it were released. At the NIPC we continue to seek partnerships which promote two-way information sharing. As Director Mueller stated in a speech on April 19, "Our top priority is still prevention." We can only prevent acts on our critical infrastructures by building an intelligence base, analyzing that information and providing timely, actionable, threat-related products to our private and public sector partners.

As for the Freedom of Information Act, many legal authorities have agreed that the Federal Government has the ability to protect information from mandatory disclosure under the current statutory framework. Indeed, in 1974 Federal courts began to hold that FOIA itself anticipates that Federal agencies do not have to release pri-

vate sector commercial or financial information if doing so would, "impair the government's ability to obtain necessary information in the future." And the FBI also has the ability to protect certain information provided by the private sector that is compiled for law enforcement purposes.

Nonetheless, the government's ability to protect information is of little value if the private sector is unwilling to provide that information in the first place. Clearly there is room for increasing the private sector's confidence level in how we will protect their information from public disclosure. stated more simply, if the private sector does not think the law is clear, then by definition it is not clear.

Therefore, we welcome the efforts of your Committee in improving information sharing, and I look forward to addressing any questions that you may have. Thank you.

Chairman LIEBERMAN. Thank you, Mr. Dick. Now Mr. Malcolm.

TESTIMONY OF JOHN G. MALCOLM,[1] DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. MALCOLM. Thank you, Senator. Mr. Chairman, Members of the Committee, I would like to thank you for this opportunity to testify about the Department of Justice's efforts to protect our Nation's critical infrastructure and about information sharing that is needed and related to its protection. It is indeed a privilege for me to appear before you today on this extremely important topic and I would commend the Committee for holding this hearing.

Since the Committee already has my slightly more lengthy written testimony, I will use the brief time that I have in my oral statement to outline the nature of the critical infrastructure protection, the information sharing problems, and the Department's current efforts to combat that problem. It is clear to the Department of Justice, as it is to this Committee, that information sharing is a serious issue and that its complexity presents significant challenges to law enforcement.

The safety of our Nation's critical infrastructure is of paramount concern to the Justice Department. As you know, the term "critical infrastructure" refers to both the physical and cyber-based resources that make up the backbone of our Nation's telecommunications, energy, transportation, water, emergency services, banking and finance, and information systems. The problem of ensuring delivery of critical infrastructure services is not new. Indeed owners and operators of critical infrastructure facilities have been managing risks associated with service disruptions for as long as they have had those facilities. However, the operational challenges of ensuring the delivery of the broad array or services that now depend upon the Internet and other information systems is a challenge that has grown exponentially in the last several years.

The burgeoning dependence of the United States infrastructure on the Internet has exposed vulnerabilities that have required the U.S. Government to mount new initiatives, to create new Federal entities, to help manage critical infrastructure protection efforts,

[1] The prepared statement of Mr. Malcolm appears in the Appendix on page 64.

and to seek prevention, response, and reconstitution solutions. The safety of our Nation is of course our first and foremost overriding objective. The Justice Department has been working across government to address infrastructure issues for several years. However, the attacks of September 11 have heightened our awareness of these issues and created a new sense of urgency.

U.S. infrastructure protection efforts are the shared responsibility of many entities, both public and private. Many of this joint effort is based upon the principle that a robust exchange of information about threats to and actual attacks on critical infrastructures is a critical element for successful infrastructure protection. The following, of course, are just a few of the entities that are dedicated to this principle: The National Infrastructure Protection Center, headed up by Mr. Dick; the Department of Justice's Computer Crime and Intellectual Property Section, which I oversee; the Information and Analysis Centers that have been referred to; the Critical Infrastructure Assurance Office, Mr. Tritak's shop; Office of Homeland Security; and the Federal Computer Incident Response Center.

To better protect critical infrastructures government and private sector must work together to communicate risks and possible solutions. Acquiring information about potential vulnerabilities from the private sector is essential. Doing so better equips us to fix deficiencies before attackers can exploit them. For example, a vulnerability in an air traffic control communication system could allow a cyber attacker to crash airplanes. That example is not entirely hypothetical. A hacker did indeed bring down the communication system at the Worcester, Massachusetts airport in 1997. After he was caught and prosecuted, and thankfully no lives were lost, nonetheless this is a sobering example.

If we concentrate our time and energy on remediation of terrorist attacks after they have occurred, we have already lost. Information is the best friend that we have for both prevention and response. And we recognize that we can protect the Nation only if the private sector feels free to share information with the government. However, industry often is reluctant to share information with the Federal Government. One reason that they give for not sharing this information is that the government may ultimately have to disclose that information under the Freedom of Information Act or FOIA. Industry is also concerned that sharing information among companies will lead to antitrust liability, or that sharing among companies or with the government will lead to other civil liabilities such as a product liability suit or shareholder suit.

Without legal protections regarding information needed by the government and which they possess in order to safeguard our infrastructure, even the most responsible civil-minded companies and individuals may hesitate before sharing such critical information, fearing that competitors may share that information and use it to their advantage. With this in mind, both the Senate and the House of Representatives have actively considered addressing this issue through legislation, and the Department appreciates the efforts of, among others, Senator Bennett, a Member of this Committee, for sponsoring such legislation.

Such a corporate good samaritan law would provide the necessary legal assurance to those parties willing to voluntarily provide sensitive information to the government that they would otherwise not provide. The Justice Department believes that the sharing of the private sector security information on critical infrastructure between the private sector entities and the Federal Government will help to avert acts that harm or threaten to harm our national security, and that this is of the utmost importance. We are prepared to work very closely with Congress to pass legislation that provides this important legal protection.

Mr. Chairman, I would again like to thank you for this opportunity to testify about our efforts. Citizens are deeply concerned about their safety and security of our country, and by addressing information sharing Congress will enhance the ability of law enforcement to fight cyber crime, terrorism and protect our infrastructure. And again, the Department stands ready to work with this Committee and with Congress to achieve those goals.

Thank you. That concludes my remarks and I look forward to answering your questions.

Chairman LIEBERMAN. Thanks, Mr. Malcolm. Mr. Tritak.

TESTIMONY OF JOHN S. TRITAK,[1] DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, U.S. DEPARTMENT OF COMMERCE

Mr. TRITAK. Thank you, Mr. Chairman, Senator Thompson, and Senator Bennett. It is an honor to be here today.

It was not too long ago that national security was something that the government did virtually on its own. The term "national economic security" used to mean largely free trade and access to markets and critical materials overseas. Now we are confronted with a unique challenge in which we have a national security problem the Federal Government cannot solve alone. National economic security now literally means defending our economy and critical infrastructures from direct attack. As Senator Bennett had indicated in his opening remarks, terrorists had indicated the economy is a target, and that followers have been urged to attack wherever vulnerabilities may exist with all means available, both conventional, nonconventional, and cyber means.

Let us be clear what their goal is, too. Their goal is to force us to turn inward and to rethink our global commitments overseas, especially in the Persian Gulf and the Middle East. Securing our homeland today is really a shared responsibility. It is protecting our way of life and the core values that we cherish. It also is going to require a clarification and maybe, in some cases, a redefinition of the respective roles of responsibility of government and industry in light of that shared responsibility. This is going to require an unprecedented level of collaboration, whereby industry must be considered and treated as a real partner. Now, I will tell you as a government person, that is going to require a cultural adjustment on both sides. But we have made it very clear that information sharing is an essential element of fostering that kind of collaboration, not just for the self interest of the companies, but for the pub-

[1] The prepared statement of Mr. Tritak appears in the Appendix on page 77.

lic interest. This actually constitutes a public good, which is why both the last administration and this one have encouraged information sharing within the respective infrastructure sectors, because availing themselves of that shared information helps them better manage the risk that they confront, and sharing between industry and government, because there are things that government can bring to this equation that industry alone cannot, and together they can help address common problems.

Moreover, information sharing is in fact occurring. There have been ISACs, as Ron Dick has mentioned and Senator Bennett has mentioned, and information sharing is taking place with the Federal Government, but it is clear from everything we have heard so far that there is a reluctance on how far that information sharing is going to go.

So I would submit to you that if I had to think through this issue in its clearest form, the question is whether the current statutory and regulatory environment is conducive to supporting a voluntary activity information sharing, which we all accept is in the public interest. And I acknowledge, and we all acknowledge, that this is not going to be easy because we may have public goods that come in conflict from time to time, i.e., FOIA exemption versus open government. I do not think we are going to solve this problem finally with a passage of legislation. Let us be clear, this is not a silver bullet. You cannot regulate or legislate trust, which is an essential ingredient to information sharing taking place, and you are going to hear in the second panel instances where that trust has evolved over time and the level of information sharing and the quality of that sharing has gone up.

Some of the newer industries are taking baby steps into information sharing, and they may take a little bit of time before information sharing in those industries fully matures. But what is clear is that if we want to encourage this voluntary activity, we need to examine the public policy and statutory environment to determine whether or not we are doing everything necessary to incentivize and encourage that activity. In the absence of a certain level of predictability and certainty, there may be an impediment to that kind of sharing.

I want to acknowledge Senator Bennett for the very good work that you have been doing, not just since September 11, but before September 11, and I think that the attempts at addressing the concerns expressed by industry are very seriously put forward and in fact are very seriously being considered by the administration. I look forward to working with you and the Committee, and I would welcome any questions you may have. Thank you.

Chairman LIEBERMAN. Thanks, Mr. Tritak. We will begin the questioning. We will have 7-minute rounds since we only have three of us here.

Last September 26, President Bush wrote to Daniel Burnham, who is the CEO of Raytheon, but wrote to him in his capacity as a leader of the National Security Communications Advisory Committee. And in the letter, which was following up on a meeting, the President says, "My administration is committed to working in partnership with the private sector to secure America's critical infrastructure, including protecting information the private sector

provides voluntarily to the Federal Government in support of critical infrastructure protection. "Accordingly, I support a narrowly-drafted exception to the Freedom of Information Act to protect information about corporations' and other organizations' vulnerabilities to information warfare and malicious hacking."

So I guess I will begin by directing it to you, Mr. Malcolm. What, if anything, has the administration done to develop the policy that the President stated in this letter, and more particularly, since the President said he supported a narrowly-drafted exception, what are the parameters, if you are at a point where you can say so, of what that narrowly-drafted exception night be?

Mr. MALCOLM. Sure. Senator, this is, of course, an evolving process, and there are several bills—Davis-Moran, Bennett-Kyl—that are pending and that are being evaluated by the administration. The administration likes a number of ideas that are in both pieces of legislation, probably prefers some of the elements of Bennett-Kyl for reasons that I will be happy to discuss with you. Nonetheless, I think it is safe to say that the administration has some concerns with all of the bills that are pending and is working to try and massage those into what the Executive Branch would consider a best practices bill.

A number of the elements that had been discussed in terms of crafting a definition of critical infrastructure information that is both large enough to get the information that the government needs to protect our critical infrastructure, while at the same token not being so large that it protects from public disclosure in the open government aspects of FOIA, protects being an over broad definition that just covers everything. The principle though of coming up with a FOIA exemption the administration believes to be a good one because, as Senator Bennett has pointed out, 85 to 90 percent of the critical infrastructure that is out there is owned and operated by the private sector. The government needs to have that information so that it can assess vulnerabilities and share appropriate information back, and they are not currently providing it. They are to InfraGard to some degree, but we need more, so there has to be a way to bridge that gap. And if a FOIA exemption, narrowly crafted, is the way to go, that is fine, whatever it takes to bridge that gap.

Chairman LIEBERMAN. Would you discuss, if you are prepared to, what some of the pluses and minuses are that you see in the various bills, which I suppose would help us understand, at this point, what "narrow" means here.

Mr. MALCOLM. I think that is fine. Again, without getting into the specifics of each legislation, I know that both pieces of legislation, for instance, have an antitrust exemption. The Executive Branch of the administration has traditionally taken the approach that an antitrust exemption is unnecessary, that a business review letter suffices.

However, that having been said, we are still studying that aspect of these bills. There are provisions in both bills about the use to which the government can put voluntarily-obtained information. Davis-Moran, for instance, I believe, prohibits the use by the government, both direct use and indirect use, of that information. Bennett-Kyl, I believe, talks about a prohibition in terms of direct use

without getting consent. The administration has some concerns about those provisions in terms of what it might do to hamper government criminal and civil enforcement efforts, some of the concerns that Senator Akaka addressed. For instance, the administration would want to make sure that any information provided to the United States could be used by the government for a criminal enforcement act.

There are incentives that are in departmental policies of long standing that we believe provide adequate incentives to turn over that information, and we are afraid that anything that is broad could allow for a document dump. It could allow for industry to just turn over information and the government would not be able to enforce its criminal laws or its civil laws. It has a similar concern in terms of prohibitions on direct or indirect use in terms of civil enforcement actions. We would probably prefer something a little more narrowly crafted in the sense that it would not tie the government's hands in either civil or criminal enforcement actions with respect to the information that it obtains. That is an idea of the direction where we are going, so we have the same concerns that Senator Akaka has about not wanting to protect too much information while at the same time giving the government the ability to engage in criminal and civil enforcement actions where appropriate.

Chairman LIEBERMAN. OK. That is a helpful response. Obviously, there is a lot of detail to it, Mr. Tritak, as we go along. Do you have any sense of timing as to when the administration would be in a position to either propose specific legislation or comment in detail on the proposals that are before us?

Mr. TRITAK. I do not, Senator. I know that is a very pressing issue. We are aware that you want to act now on this matter. We want you to act on this issue, and we want to strike while the iron is hot, so I will certainly relay your concerns about the timing and get back to you.

Chairman LIEBERMAN. I appreciate that. Mr. Tritak, you talked about trust, which I agree with you, it is a very important element here in that the kind of exemption we are talking about could create a foundation of trust that sensitive information shared with the government will be secured. I want to ask you to talk for a moment about two aspects of that. The first is, just for the record, on what basis you conclude that a new FOIA exemption could actually make a significant contribution to information sharing. And as part of that, if you would consider what one of the witnesses, by submitted testimony, will say on the second panel, which is some skepticism that all information that the government would want to have will in fact be shared by the private sector, even with a FOIA exemption, because of concern about the proprietary, private, etc. nature of it.

Mr. TRITAK. I would be happy to. Senator, first I will talk to the first question—about what would it actually do. We have to take into account that, for example, with the FOIA laws, they predate this problem. They were on the books long before this issue of information sharing to advance critical infrastructure protection came up.

Chairman LIEBERMAN. Right.

Mr. TRITAK. We have been trying to encourage industry to take proactive voluntary steps to do things they are not required to do right now. The clarifying of FOIA, and I think what Senator Bennett said is exactly the right way, you could approach in one of two ways. You can say that the current environment, if you are very careful and you watch out, the existing exemptions will cover any concerns that may arise regarding FOIA, not to worry.

The response we have usually heard in those instances was, "Well, but that makes us have to second guess our actions. That makes us have to second guess what we are trying to do here." And also to be clear, the kind of legislation we are looking at and the kind of trust we are trying to create must take place in a dynamic environment. It is not a set piece exchange where you take a piece of information, you hand it over, it gets considered, and it comes back. Information must flow all the time and at different levels. You cannot stop the process for every little bit of informatin to determine whether it is covered under FOIA. It is very interesting that you should mention the NSCAC as the letter for the President because in fact they have had 20 years of information sharing. And the idea here is, is that companies believe more can be done if this environment is more clear and predictable in terms of the complication of FOIA.

Now, I think Ron would attest that when it comes to an actual event, an incident in real time, there is a lot of sharing that goes on. What we are trying to do here is encourage proactive sharing before incidents occur and in a dynamic setting so that companies will actually take preventive and proactive measures. And so I think that is what the trust, along with the right legislative framework, will foster.

In terms of the skepticism, I want to make very clear, as I said before, that FOIA alone is not going to be the silver bullet to information sharing. You are not going to get an avalanche of information being shared with the government just because you have this bill piece. What it does, in my judgment, is create an environment that is conducive to that kind of sharing and send a signal to industry that, if you engage in this kind of activity, you will be protected against certain types of disclosures.

Chairman LIEBERMAN. Thanks, Mr. Tritak, I apreciate your answer.

Senator Thompson and I are smiling because, I do not know whether it is the quality of your answer or staff deference to the Chairman, but the time available to me seems to be growing instead of shrinking. [Laughter.]

Senator THOMPSON. It is the power of the Chair.

Chairman LIEBERMAN. Must be. But I am going to have to declare that my time is over, and yield to Senator Thompson.

Senator THOMPSON. Thank you very much, Mr. Chairman.

I think that a valid distinction to make here is that under FOIA as it exists, although the government may be able to withhold certain information that we are talking about here, it is discretionary with the government, and the distinction between that and this bill would be that it would be mandatory. Is that a valid distinction to make, it would be incumbent upon the government to withhold it and would have no discretion?

Mr. MALCOLM. My understanding, Senator, is that there is some discretion in FOIA as it currently exists except as it pertains to trade secrets.

Senator THOMPSON. OK. I think that, Mr. Malcolm, it seems to me like you are on the right track and asking the right questions about this. Many of us are not as steeped in this subject as Senator Bennett and some others are. But in looking at it I would think that the first thing that you—although clearly we need to do something in this direction if it is going to help. One of the first things that you would want to look at is whether or not it would allow a company that perhaps is in a little trouble and sees some vulnerability, to protect itself just strictly for the purpose of protecting itself to do the document dump.

Mr. MALCOLM. Right.

Senator THOMPSON. And the definitions, as they are currently drafted, provides protection of sharing of information concerning critical infrastructure which it defines as physical and cyber-based systems and services essential to the national defense, government or economy of the United States, including systems essential for telecommunications, electric, oil, gas, etc. It seems to me like this is very broad language and could cover anything from farming to automobile production. And the question would be whether or not if a company was doing a very poor job, deliberately doing a very poor job to save money and protecting its critical infrastructure, and it saw there were some rumblings out there concerning civil lawsuits or the government beginning to take a look at it, it could get a bunch of stuff to you in a hurry and totally protect itself, and keep you, for example, from conducting a civil action against them. I would think that would be something that nobody would want, and I am not sure how you address that, but I think you are asking the right questions, and that is something that should be addressed.

In addition, we are operating under the assumption here—and I assume we will get more of this from the next panel—that information is really being withheld. I think it is important to create a public record for a need for this bill. It stands to reason logically that if there is some vulnerability out there and sharing information, that it is less likely to be shared, but do you really hear instances from industry or others where they are saying that they are really restrained somewhat or afraid to share information for the reasons that we have discussed, any of you?

Mr. TRITAK. Well, I will just speak for myself. I have been told that precisely, particularly when you are talking about potential systemic problems and vulnerabilities—that there is a real reluctance to share information about those things without better understanding about whether or not you will be protected under FOIA. We are hearing this across a number of sectors.

Mr. DICK. Where this comes into play, as was mentioned, when we get into a crisis like with Code Red or Nimda or any of those, the private sector comes forward very, very willingly.

Where I think the enhancements need to occur is from the predictive and strategic components, wherein information is shared on a routine basis so that we can be out in front, if you will, of the vulnerabilities so as to share with the private sector what action-

able things they can do to prevent them from becoming victims, and that is the kind of thing that needs to occur on a daily basis.

For example, during the events of September 11, one of the things that we did very routinely with the Information Sharing and Analysis Center is share physical threat information. We did that for two reasons. One, obviously, is prevention and protection, but two, as we got threats, let us say to the oil and gas industry, only the oil and gas industry experts know that industry from an expert level so as to assess, well, is the threat as described even viable to the oil and gas industry, so as to determine is it a valid threat? So we have to have the ability to share at times even classified information to the private sector to assess that threat and then determine what are the right actions to be taken.

Senator THOMPSON. Right.

Mr. MALCOLM. Senator, if I may, I just think it is fair to say that to some degree we do not know what we do not know. We need to know it and we need to know it now. Obviously, 85 to 90 percent of the critical infrastructure is owned and operated by private sector. When threats happen or when incidents happen, all of a sudden information which the government did not know about comes forth. We need to have that information now so that we can deal with it prophylactically and have that information at hand if, God forbid, does happen, track down these perpetrators quickly before they repeat their act.

Senator THOMPSON. One of the critical parts of all of this is private industry cooperation with each other. The bill addresses the antitrust aspect of it. And I am wondering whether or not, even if that is taken care of, that there will still be a concern from a competitive standpoint with regard to industry sharing information with each other, they would be allowed to do that. The government may not come down on them for that, but does that in any way—of course this bill, I do not think, addresses that and perhaps cannot. I am just thinking from a practical standpoint that we still have a problem. I think that was a part of the Presidential Directive 63, trying to get industry to work with each other and the government working with industry, etc. It looks to me like this would still be a concern there in the private industry with sharing information one company with another strictly from a competitive standpoint. Do you have any thoughts on that at all?

Mr. DICK. Senator, it is a valid concern. It is one we hear fairly routinely, particularly in the information technology arena. However, I think what is—as I talked about in my statement, you see with the number of Information Sharing and Analysis Centers that are being created, with the amount of information that is being shared internally within those organizations. There is a building of trust, as Mr. Malcolm talked about and I talked about too, amongst them. That does not happen overnight, and as was indicated earlier, you are not going to legislate that. Only with time and experience, and that there is value added to the bottom line of these companies through sharing information and reducing the threat is that going to come to fruition. But I think there are very positive first steps that we have made and this Committee can make, by providing the assurances to the private sector that we will minimize the harm that could occur.

Mr. MALCOLM. Senator, if I may answer your question briefly, I think that even if you had an antitrust exemption, that is not going to do away with antitrust lawsuits. I mean it is going to then be a question of did the competitors who sat down in the room together extend beyond the bounds of the information that they were supposed to discuss?

Senator THOMPSON. If they only did the things that the exemption provides them with in this bill, they would not have had any antitrust problem anyway.

Mr. MALCOLM. That is right, and that is, again, when we talked about ways in which we are looking at this possibly narrowing it, again, these issues have been dealt with in the past. There is a business review letter once the government has issued a business review letter, which it can in particular circumstances actually do fairly quickly. There has never been an enforcement or antitrust action brought following the issuance of a business review letter, and I think that it might provide some protection on the margins in terms of people feeling comfortable walking into a room together, but in terms of whether they extend beyond the bounds of just talking about critical infrastructure information and getting to pricing and whatnot, that is still going to lead to allegations and possible lawsuits.

Senator THOMPSON. Thank you very much.

Chairman LIEBERMAN. Thanks, Senator Thompson. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. Good morning.

Chairman LIEBERMAN. Good morning.

Senator CARPER. To our witnesses and guests, thanks for coming this morning. It is my third Committee hearing I have been to, so I apologize for missing most of what you said. I just arrived when Senator Lieberman was questioning you during his first hour of questioning. [Laughter.]

I think you have some comments on legislation that maybe Senator Bennett has introduced, and I am not aware of what you had to say about it. Do you have anything positive that you might share with us about the legislation that he has introduced, just each of you?

Mr. MALCOLM. Specifically about Senator Bennett's legislation, that fact that he has not charged across the desk and at me I think is indicative of the fact that we have said some very positive things about the legislation.

Senator CARPER. Just share a couple of thoughts you had with me.

Mr. MALCOLM. Certainly. It provides, for instance, with the government to be able to use independently obtained information without restriction, certainly in terms of not prohibiting the government's use of indirectly or derivatively obtained information in a criminal or civil enforcement action. That is a very good thing. I did take some issuance with Senator Bennett in terms of saying that perhaps even a direct preclusion by the government in terms of the use of information might not be in order, but nonetheless, in terms of a thrust of bridging the gap between private industry

and the government in terms of getting that information, we are well down the road and in the right direction with Bennett-Kyl.

Senator CARPER. Anyone else? Mr. Dick, do you have any thoughts?

Mr. DICK. We have had a number of discussions, my staff with Senator Bennett's staff, and are well aware of the legislation, and frankly, are supportive of many aspects of it. As I talked about in my opening statement, we believe that there are sufficient provisions in the FOIA now to protect information that is provided to us. But it really does not matter. If the private sector does not believe it, and does not feel comfortable with it, then we need to provide them those assurances that make them feel that a partnership with the government is worthwhile and is value added to them, and Senator Bennett's bill as a whole does that.

Senator CARPER. Any changes you would recommend that we might consider in his legislation? We are usually reluctant to try to amend his legislation, but maybe one or two.

Mr. DICK. I would defer back to my esteemed colleague, Mr. Malcolm, with the Department of Justice in that regard.

Mr. MALCOLM. Well, one of them I have discussed already, Senator Carper, which has to do with direct use by the government in a civil enforcement action. I think that that ties the government's hands inappropriately, but I am pleased to see that it is a direct use prohibition and not an indirect use prohibition.

Certainly if we are going to tie the government's hands at all, I would prefer seeing, say, a provision in there that allows an agency head to designate which section of an agency is to receive this voluntary information so that other branches of the government can pursue whatever leads it wants to, and use any information that it obtains in a full and unfettered measure. Again, independently obtained information is in there. I forget whether Bennett-Kyl has a requirement that the company said that it is voluntarily providing this information and intends for it to be confidential, but I think that is a good thing.

As I recall, Bennett-Kyl, although I may be getting my bills confused, allows for oral submissions to get FOIA protection from the administration's perspective. Again, while we are still mulling this over, I think, to use a non-legal term, it is a little bit loosey-goosey in terms of it does not make clear what information we are talking about, how it is to be provided, and certainly the administration would prefer to see something in which any oral submission were reduced to writing. Those are just a few things.

Senator CARPER. All right, thanks.

Mr. Tritak, tell us a little bit about your wife.

Mr. TRITAK. I am not sure she is here.

Senator CARPER. She is not. I do not see her. I do not know if my colleagues know this, but whenever——

Chairman LIEBERMAN. You have a right of privacy, Mr. Tritak. [Laughter.]

Senator CARPER. No, I think he surrendered that. When the roll is called, not up yonder but in the Senate, there are a couple of roll clerks who call the roll, and among the people who do that are Mr. Tritak's wife. Katie, right?

Mr. TRITAK. Katie.

Senator CARPER. And then while I was presiding yesterday, she mentioned to me, she says, "My husband is going to"—I said, "Is this your first husband, Katie?" [Laughter.]

She said, "He is going to be testifying tomorrow before your Committee." And I said I would be sure to remember to thank you for sharing your wife with us. She does a great job. She keeps us all straight and on a very short leash. It is very nice to meet you.

Let me just ask you a question, and I do not care who really jumps into this one, but take a minute and tell us how you work together, how do your agencies work together in the information sharing program?

Mr. TRITAK. I would like to actually restate that. We have very clear roles and responsibilities and I would say that our working relationship has actually been quite excellent over the last few years. Mr. Dick and I probably talk at least once a week.

My own rule generally, although not in particular detail, is to try to focus on the front end of getting industry to see this as a business case. We have been talking about this as a national security issue. I actually think there is a business case. I think it is a matter of corporate governance. I think this is something that is important for them in terms of their own self interest as well as the interest of the Nation. And the extent to which we can translate the homeland security proposition into a business case, I think we begin to advance greater corporate action. There is a lot of corporate citizenship that you are seeing now. There is a lot of "wanting to do the right thing," but it is also helpful to understand that this can actually affect the bottom line. This is actually something that advances and is in the interest of their shareholders, as well in their industry, in general.

Having achieved that, my goal is frankly to find "clients" for Ron Dick, who then picks up that case and develops the operational relationships in terms of the specifics of information sharing, working with the lead agencies, working with the ISACs who you will hear from in a few minutes. So I think that is how I certainly see the matter.

Mr. DICK. Continuing on with that theme, with the recent Executive Order by President Bush and the creation of the President's Critical Infrastructure Protection Board under Dick Clark has even further solidified that spirit of cooperation within the government. The intent of the board creation, in my estimation, is to raise the level of security and insofar as the government systems are concerned from the CIO level actually to the heads of the agencies themselves. And the intent of the board is to make the government, if you will, if possible, a model to the private sector as to how information security should occur as well as information should be shared amongst agencies. We have created a number of committees. I am on the board and chair of a couple of them, insofar as working within the government and with the private sector to develop contingency plans as to how we will respond to an incident.

Frankly, having been in this town for a number of years myself, the environment and the people that are heading up this effort are truly unique insofar as our willingness to move the ball forward, if you will. And the private sector, in my estimation, through Har-

ris Miller and some of the others, Alan Paller, are frankly coming out front, too, to try and figure this out.

Mr. MALCOLM. I have nothing really to add, Senator, other than, for instance, the attorneys that I oversee in the Computer Crime and Intellectual Property Section have daily, sometimes hourly contact with the National Infrastructure Protection Center, and then also through dealing on various subcommittees with the President's Critical Infrastructure Protection Board we also have dealings with Mr. Tritak's shop among others. So it works well within government.

Senator CARPER. Well, that is encouraging. Thank you for sharing that with us.

Mr. Chairman, if my time had not expired, I would ask Mr. Dick and Mr. Malcolm to report on their wives as well. [Laughter.]

Chairman LIEBERMAN. They and I are happy that your time has expired. [Laughter.]

Senator CARPER. I would say to Mr. Tritak, it is a privilege serving with your wife, and we are grateful for that opportunity and for the testimony of each of you today. Thank you.

Chairman LIEBERMAN. I think we can all agree on that. Thanks, Senator Carper. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman. If I can just put a slight historical note here. Mr. Malcolm, considering the initial reaction of the Justice Department to my bill and your comments here, I can say to my colleagues that we have moved a long way. [Laughter.]

Because the initial reaction was not only no, but no, on just about everything, and I am grateful to you and your colleagues at the Department, that you have been willing to enter into a dialog and we have been able to move to the point where you are able to make the statements that you have been making here. I think it demonstrates great progress. And I come back to a comment that Mr. Tritak made, which I think summarizes very clearly the problem we have here, when he says this is going to require a significant cultural adjustment on both sides. We have had grow up in this country the adversarial, if you will, relationship between government and industry. Maybe it comes from the legal world where everything is decided by advocates on two sides who fight it out and then presumably the truth comes as a result of this clash.

This is not something that lends itself to the adversarial attitude. This is something that requires a complete cultural adjustment. Industry automatically assumes that anything they share with the government will be used against them. There is an unspoken Miranda attitude that anything I tell the Feds, they are going to turn around, even if it is totally benign, they are going to look for some way for some regulator to find me or damage me in some other way. And some regulators have the attitude, unfortunately, that anybody who goes into business in the first place is automatically morally suspect, that if they had real morals they would teach. [Laughter.]

Or come to work for the government. And we have got to break down those cultural attitudes on both sides and recognize, as this hearing has, that our country is under threat here, and people who wish us ill will take advantage of the seams that are created by

these cultural attitudes, and we have got to see to it that our protection of our critical infrastructure becomes truly seamless between government and industry, and there is an attitude of trust for sharing of information.

Now, let me get directly to the issue that Senator Thompson raised with you, Mr. Malcolm. Do you see anything in my bill that would allow someone to deliberately break the law and then try to cover that by some kind of document dump?

Mr. MALCOLM. Well, I will answer you question this way, Senator—and I am not meaning to be evasive—I believe the intent of your bill, for instance, is not to preclude the government from using the information in terms of a criminal prosecution, although I believe that intent, assuming that is your intent, should be spelled out perhaps a little tighter. But assuming that is your intent, that any information provided voluntarily or otherwise to the government they can direct use of it, derivative use of it in terms of a criminal prosecution, then the answer to your question will be no.

In terms of a civil enforcement action—and of course there are many elements that go into a criminal prosecution which may or may not be appropriate. Sometimes you want to take, say, environmental cleanup efforts or any civil enforcement action that is not a criminal prosecution, there is nothing in your bill that I see that prevents that action from going forward. There are things in the bill that make such an action more difficult in terms of precluding direct use of the information that is voluntarily submitted, and of course, that does leave it to a court to determine when you cross the line between direct use and indirect or derivative use. So there is some gray area on the margins of what the term "direct use" means, so it is possible that a company say could be negligent in its maintenance of manufacture of some component that deals with critical infrastructure could get some noise out there that something bad is about to happen that might subject the company to civil liability, could do a document dump on the government, and the government would be circumscribed to some degree in terms of its ability to use that information in a civil enforcement action.

Senator BENNETT. Not being a prosecutor and not being burdened with a legal education—— [Laughter.]

My common sense reaction would be if we were getting—I put myself now in the position of the government. If we were getting a pattern of information from an industry, say a dozen different companies were saying, "This is what is happening, this is what is happening, and so on," and one company does a document dump in which there is an indication that something is wrong with their maintenance, it would seem to me, if I were sitting in that situation, here is a red flag that these people are not giving us legitimate information for legitimate purposes. These people have something serious in mind that they are trying to protect and would make me examine their submission far more than I otherwise would. If I were the CEO of a company, and I have been, and somebody in my legal department were to come and say, "Hey, we can cover this. This is what we would do." In the first place, I would not tolerate that in any company that I was running, but if someone were to come to me with that idea that this is how we are going to cover this, I would say, "You are up in the night here, this

is crazy. Fix the problem. Disclose what we need to disclose to help deal with the critical infrastructure thing, but do not think that the Feds are stupid enough to overlook what you are trying to cover here."

But that having been said, obviously we have the intention you are imputing to us. We do not want, under any circumstances to say that the sharing of information with the government will provide cover for illegal activity or that it will provide cover that somebody in a civil suit could not file a legitimate subpoena for that information.

Mr. MALCOLM. The only thing that I am saying, Senator, and we are not really disagreeing with each other, we are certainly foursquare together with respect to a criminal prosecution. With respect to a civil enforcement action, if you assume you are in the perspective of the government and the evidence has been dumped upon you, if you have say a bad faith exclusion for dumping documents, that puts you into the difficult position of having an evidentiary hearing of sorts to determine what was in the minds of the people who dumped the documents. Were they doing this in bad faith because they realized that their vulnerabilities that were of their own making were about to come to light? Or were they dumping it because they realized that they had these vulnerabilities, whether they should have fixed them or not fixed them. That could harm the government and harm the citizenry. Those are evidentiary issues.

All I am saying, in terms of impeding an effort, is if you are in the position of the government and you receive this information, and it is now not FOIA-able, because this now fits within an exemption, so you are largely relying on the government to take an appropriate civil remedial action, there are constraints within the bill that you drafted as to what you can do with that information and how far the direct use extends into information we get. I am not saying it is not doable, because for example, in the hypothetical that you used, you said, well, there are other companies out there that are making rumblings about what bad company is doing. Well, if you get the information from those other companies, it is independently derived, you are in the clear. But if the crux of the information that you have received is from a company that has done the document dump, you then are in the area of trying to figure out or have a judge figure out what motivated the company in terms of making that submission, and you are also in the area in terms of saying to what use can you put the information that has been provided, and again, it is our belief that there are already benefits that a company can get by providing the information. There is a policy that gives favorable consideration for voluntary disclosures in terms of criminal prosecution and civil enforcement actions. That should be enough, and that the government's hands should not be tied in terms of taking appropriate civil enforcement actions, particularly since that information is not going to be FOIA-able and will probably be protected from other civil lawsuits by private organizations.

Senator BENNETT. If I can just very quickly, Mr. Chairman, on this whole question of a cultural attitude change, it may very well be that the very thing that the head of Homeland Security of the

Department of Defense needs to know in the face of an attack is the particular vulnerability that this one company might otherwise not disclose. So I am very sympathetic to what you are saying about the need to see to it that people do not get off the hook, but let us not lose sight in our effort to hang onto that, of the possibility that a terrorist has discovered that this company is the most vulnerable because of bad maintenance or whatever, and is moving in that direction. And if the government does not get that information, we could all be sitting here looking at each other after an attack, saying, "Gee, we wish we had paid equal attention."

Thank you very much.

Chairman LIEBERMAN. Thank you, Senator Bennett.

This is an important line of questioning, and before we move on to the next panel, I want to just take it one step further, and in fairness give my colleagues an opportunity to ask another question also. And this is about the effect on the regulatory process—we have talked about civil and criminal actions—both the authority of the government and the responsibility of private entities under the regulatory process. So I would guess we will hear on the second panel a concern that has been expressed by the environmental community about what an exemption under FOIA as proposed by Senator Bennett's legislation would do to a company's obligations under the right-to-know laws, where they are providing information about environmental health or safety risks and problems, and then that information is made available by the government to the public. There are concerns that the exemptions granted here might give the companies a ground for withholding some of the information that otherwise would be public. Similarly, there is a concern that if a company voluntarily submits the information, receives a FOIA exemption, and then the government decides—perhaps the Justice Department—that the information should be considered for instance in deciding whether to grant a permit, an environmental permit or some other permit for the facility, whether the information has to continue to be kept secret.

So my question would be whether you think that those fears are justified, and if so, is there a way to handle them in this legislation?

Mr. MALCOLM. That is an excellent question, Senator, and in part you are going beyond my ken of expertise, but I will answer it as best I can. And this goes back actually to the point that Senator Bennett just made at the end, which is that we are trying to come up with a fine balancing act that incentivizes companies to give over this information which is desperately and vitally needed by the United States, while at the same time not giving them an ability to, if you will, hide their misdeeds and to get away. And this is a balancing act.

In terms of the first part of your question, which I took to mean that, gee, if we were to create such an exemption, that would give a company an excuse to withhold information that it otherwise——

Chairman LIEBERMAN. That they would otherwise have to make public under right-to-know laws.

Mr. MALCOLM. While I would like to give that matter more thought and perhaps my answer might change, I will say at the risk of shooting from the hip, that I think that concern is probably

somewhat exaggerated for two reasons, which is, one any exemption that would be created here I do not believe would take precedence or in any way overrule any other requirements that the company might have. So if it is required under some other regulation to put forth information, I do not think that the company could all of a sudden come back and say, well, I do not have to comply with that regulation because of this FOIA exemption.

As well, with respect to private parties' abilities to obtain information, I think we need to be clear, one, this is information nobody would have had but for the voluntary disclosure, and two, it only prevents private parties from one avenue of getting this information, and that is through a FOIA request. It is not taking precedence in any way of any other avenue that civil litigants or interested parties have at their disposal and use frequently to great effect to get information from private industry. It is just saying that among your arsenal of ways of obtaining information, this quiver is being taken out of your arsenal.

Now, you had a second part to your question which dealt with any possible effects on, if a voluntary disclosure is made in terms of the government's ability to share that information in a regulatory environment, and I am afraid, Senator, that really is sort of beyond my expertise.

Chairman LIEBERMAN. I understand. I would ask you to think about that, and I appreciate your answer to the first part, and as the administration formulates its exact or detailed position on this question, I hope you will keep it in mind that it may be that we can handle this with a simple explicit reassurance in the legislation that there is no intention here to override any other responsibilities that anyone otherwise would have had under other laws.

Do any of my colleagues wish to ask another question of this panel?

Senator THOMPSON. Mr. Chairman, along that line, it would seem—I am looking at a summary of the bill here that says the voluntarily shared information can only be used for the purposes of this act. And so I would assume that the purposes of this act would not include environmental enforcement or anything like that. And without written consent, cannot be used by any Federal, State or local authority, or any third party in any civil action. So I think, as you indicated, there is nothing in here that would prohibit using the very information the company gives you to carry out a criminal action against the company. So you can use the information in a criminal proceeding, I would assume, although you have got to have some company lawyer assuring the boss that there is no criminal exposure when they turn that information over, a little practical matter there. But assuming they do, you can use it directly.

And in a civil action you can use information derived from other sources. You just cannot use the information that the particular company sent you. But then you would have to carry the burden of proving that you are basing your enforcement action on that other material and not this particular information this company sent you. Somewhat like when a Federal prosecutor gets into sometimes when we have hearings, and he has to prove that he is building his case based on things other than what was on national tele-

vision every night for a week, and he did not get any information there that he used. There is no fruit of the poisonous tree and all that. So there are some practical impediments there.

But getting back to what Senator Bennett said we should not forget that what we are doing here is pretty important and there are some tradeoffs, it seems to me. There is no way that we can avoid some potentially, not the best kind of result. If you have got a company that is supposed to be running a nuclear reactor and they are doing a shoddy job of it, is it not best maybe that we know they are doing a shoddy job of it, even if nobody can sue them? [Laughter.]

On the other hand, what if they persist in doing a shoddy job and refuse to do anything about it; what does that leave you?

I think you are on the right track. You are asking the right questions, and I think that hopefully we will wisely make those tradeoffs. Thank you.

Chairman LIEBERMAN. Thanks, Senator Thompson.

Senator Carper, do you have another question?

Senator CARPER. I think I have done enough damage with this panel. Thank you. [Laughter.]

Chairman LIEBERMAN. Senator Bennett.

Senator BENNETT. Well, I think this has been a very useful discussion, and certainly we stand ready to make the kinds of clarifications Mr. Malcolm is talking about, because it was never the intent and never should be, that this desire to get information should be used in any way to cover any illegal or improper activity. But the one thing that I want to stress one more time that has already been mentioned, but just to make sure we do not lose sight of it, without the passage of some legislation along the lines that I have proposed, in all probability the information that we are talking about will not be available to anybody anyway. We are not talking about something that is a new protection because the ultimate protection, absent our legislation, is the lawyer and the CEO sitting down and saying, "We are not going to tell anybody about any of this, so that nobody knows. The government does not know. Competitors do not know. A potential litigant in the environmental community or anyplace else does not know because we are just not going to let anybody know about this." And if the legislation passes and then the CEO says, "You know, this is potentially a serious problem, and we can let this out knowing that the effect on our business will be exactly the same as if we do not let it out." That strikes me as a positive good for the government to have. So let us keep understanding in all of this discussion that we are talking about information that would otherwise not be available to anybody.

Chairman LIEBERMAN. Thanks very much, Senator Bennett.

Gentlemen, thank you. I agree with Senator Bennett, it has been a very helpful discussion, and we look forward, as soon as possible to the administration's recommendations to us. Thank you.

We will call the second panel now. Michehl Gent, who is the President and Chief Executive Officer of North American Electric Reliability Council; Harris Miller, President of the Information Technology Association of America; Alan Paller, Director of Research at the SANS Institute; Ty R. Sagalow, a Board Member, Fi-

nancial Services ISAC, and Executive Vice President of eBusiness Risk Solutions, American International Group; David L. Sobel, General Counsel, Electronic Privacy Information Center; and Rena I. Steinzor, Academic Fellow, Natural Resources Defense Council and also more particularly a Professor at the University of Maryland School of Law.

We thank you all for being here. I know you have been here to hear the first panel, and we look forward to your help for us as we try to grapple with this serious matter and balance the national values that are involved.

Again I will say to this panel, that your prepared written statements submitted to the Committee will be printed in full in the record, and we would ask you to now proceed for an opening 5-minute statement. Mr. Gent.

TESTIMONY OF MICHEHL R. GENT,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Mr. GENT. Thank you Chairman Lieberman, Senator Thompson, and Committee Members for this opportunity to testify on information sharing in the electric utility industry, and information sharing between industry and government as it relates to critical infrastructure protection.

Because of electricity's unique physical properties and its uniquely important role in our lives, the electric utility industry operates in a constant state of readiness. The bulk electric system is comprised of three huge integrated synchronous networks that depend instantly and always on coordination, cooperation, and communication among electric system operators. We treat preparation for acts of terrorism the same way we deal with the potential loss of a power plant or transmission line. We have trained people, facilities and procedures in place to handle these contingencies. What we lack are security clearances for key electric industry personnel to be able to receive and evaluation classified threat information. We also lack the equipment that would allow us to communicate by voice over secure channels with people that have these clearances.

In my written statement I have outlined our very good working relationship with the U.S. Government, the FBI, the National Infrastructure Protection Center, the Department of Energy, the Critical Infrastructure Assurance Office and others. We have successfully managed a number of very difficult challenges including Y2K and the terrible events of this past September. I commend the NIPC and the DOE specifically for the way they have conducted themselves and their programs.

At the heart of our success is our commitment to working with the FBI. We made this commitment nearly 15 years ago, and the trust in each other that we have built over the years has carried over into the NIPC. The word "trust", as you have heard here earlier today is a very important word to us. Without trust none of these programs will work. We are proud of our relationship with the NIPC and the DOE. However, this strong relationship could be much better, could be stronger. Trust alone is not enough to allow

[1] The prepeared statement of Mr. Gent appears in the Appendix on page 81.

us to do the additional things that are needed to prepare for future possible terrorist attacks. To be able to share specific information with the government we need to have some assurances that this critical information will be protected. To be able to share specific vulnerability information within our industry and with other industries to do joint assessments of inter-sector vulnerabilities, we need to have targeted protection from antitrust laws. We therefore support S. 1456 introduced by Senator Bennett.

The electric utility industry is building on the trust of one another that we developed in its Y2K effort. We are approaching critical infrastructure protection similar to the way we dealt with Y2K. We have an all-industry organization called the Critical Infrastructure Protection Advisory Group. In my testimony I have outlined the scope and activities of that group. It is very active and we are very proud of the progress they are making.

Our Information Sharing and Analysis Center, or ISAC, gets lots of acclaim. We have had a lot of practice and we have been doing this information gathering, analysis, and dissemination for decades. We did not get much attention before because most people have not given too much thought about what it really takes to keep the lights on. Adding cyber threat awareness to our physical threat analysis programs was a natural. Physical and cyber activities are becoming increasingly entwined.

We believe that our electric industry's experience is a great formula for success and an example of how an industry organization can best serve the industry that supports it. To take the next steps and to deal in greater detail with the combined threats of physical and cyber terrorism, our industry needs an even greater ability to share information within the private sector and with the government.

In summary here are my recommendations. We need to provide a way of sponsoring agencies such as the FBI and DOE, to increase the number of industry personnel with security clearances. Private industry input is needed for any credible vulnerability assessment. We need to provide inexpensive, effective, and secure communication tools for industry participants that participate in these infrastructure ISACs. We need to provide limited specific exemptions from Freedom of Information Act restrictions for certain sensitive information shared by the private sector with the Federal Government. We need to provide narrow antitrust exemptions for certain related information sharing activities within the industry. We believe that S. 1456 does achieve this result.

And finally, we need to adopt the reliability legislation that has been passed by the Senate as part of the comprehensive energy bill.

Again I thank you for this opportunity. I look forward to your questions at the end of the panel.

Chairman LIEBERMAN. Thanks, Mr. Gent. Mr. Miller, please proceed.

TESTIMONY OF HARRIS N. MILLER,[1] PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. MILLER. Thank you very much, Mr. Chairman. On behalf of the more than 500 members of the Information Technology Association of America, I am very pleased to be here in front of you. I know my 5 minutes is going to go quickly, but I just want to say a couple of personal things.

First of all, Senator Thompson will be sorely missed when he retires at the end of this Congress. I am not sure I am going to have another opportunity to testify before this Committee, but his leadership on information technology issues and bringing information technology to the government has been quite remarkable and we really appreciate his leadership and that of the staff.

Chairman LIEBERMAN. I agree, and I will be sure to tell him. This is one of those rare cases in Washington where you say something nice about a person when he is not in the room. [Laughter.]

So that is even more sincere.

Mr. MILLER. Thank you, Mr. Chairman. Second, it is once again a pleasure to work very closely with Senator Bennett, whose leadership on the Y2K has been continued on this issue and we appreciate it.

And third, Mr. Chairman, one of my senior staff recently found a bestseller called "The Power Broker" authored by you——

Chairman LIEBERMAN. Your testimony is becoming more and more impressive as you go forward. [Laughter.]

Mr. MILLER. And my staffer asked if you would agree to sign this. We promise not to go out on the eBay auction site. So thank you, Mr. Chairman.

Last, but not least, I did bring my general counsel, Joe Tasker with me. While you were studying at the law school at Yale, I was up the street at the political science department, so if this gets too technical I may turn to my general counsel to help.

Basically, I want to make just a couple of important points today. First of all, we strongly endorse the Bennett-Kyl bill, and certainly none of the suggested changes made by Mr. Malcolm on behalf of the Justice Department would give us any heartburn if the primary sponsor feels that those are acceptable. So the kind of narrowing that the Justice Department is suggesting sounds quite reasonable if Senator Bennett, Senator Kyl, and the House sponsors also agree, so we can certainly go along with that.

Basically three simple messages I want to leave you with. The cyber security threats are substantial and growing. Second, information sharing requires tremendous trust, and that was also discussed in the first panel. And third, we think that passage of this legislation is essential if we are going to move along that trust quotient that is necessary.

In terms of the growing threat, I have a lot of data in my written submission, but let me just make one simple point. We now believe that a new virus or worm is being written and unleased out there every 5 minutes, so just while I am testifying before your panel, we are going to have a new virus or worm out there. In the 2 hours

[1] The prepared statement of Mr. Miller with attachments appears in the Appendix on page 94.

of this hearing you are going to have a couple of dozen new viruse worms out there. So the threat is enormous. It is growing, and the attention that this Congress can put on this issue is very important.

We know that most citizens are much more scared of physical threats and biological threats than they are of cyber threats, but as Senator Bennett has so eloquently stated on many occasions, the worst-case scenario is really the combination of a physical threat or a bio threat with a cyber threat, and because our society, our government and our economy are so dependent on our cyber network, the attention this Committee and this Congress is paying to cyber threats and that the administration is paying is absolutely essential.

Well, if the threat is so real, what is the problem about information sharing? Well, we all remember the old adage "Macy's doesn't tell Gimbel's." Well, it is particularly true, as Mr. Dick suggested in the previous panel in the information technology industry. We are a very competitive industry, and as the head of a trade association, I can tell you how difficult it is to get them to share information, and in particular, Macy's and Gimbel's do not go tell the cops. That just is not the way it is done. But yet as the first panel pointed out and you pointed out in your opening statement, Mr. Chairman, that is essential if we are going to deal with this threat. We need to get a situation where we are sharing the information. So how do we do it? How do we get beyond the business as usual mentality that these organizations have?

Well, Senator Akaka mentioned that "terrible" acronym, ISAC, the Information Sharing Analysis Centers, but those are critical. Let me be clear what this is. These are closed communities. Now you may say, "Why do you need a closed community?" Because we are dealing with, by definition, sensitive and confidential information, just as the government has classified internal information that they do not want to share with the public or with potential terrorists or criminals, similarly the industry has those issues. And so we are creating with these Information Sharing Analysis Centers which are closed community environments.

So the first challenge is to get the ISAC members themselves to share information. As one who was instrumental in setting up the IT ISAC, for example, I can tell you that is still difficult. We are still taking baby steps even though the organization was formally announced almost 14 months ago and has been in full operation for over 8 months. It is very tough to get people to share this kind of sensitive proprietary confidential information even though they know in some sense it is the right thing to do, because not only, as was pointed out in the previous panel, do you have to see the return on investment, you also have to be sure there is no enormous downside, and that downside of that public disclosure is perhaps one of the biggest threats to that.

And then we have to move on, as Mr. Gent just said in his comments, to sharing across the ISACs, so we have that kind of sharing. There are institutions being created to do that. There are institutions that already exist such as the Partnership for Critical Infrastructure Security that encourage that, but we really need to advance that.

And then of course the sharing with the government, which is really what Senator Kyl and Senator Bennett's bill is all about; how do we move beyond simply sharing within industry, again, sensitive information before events occur? And we believe that this information sharing will be accelerated if key executives, and particularly the lawyers who are the gatekeepers here, are willing to allow their companies to share information without the threat to FOIA.

We certainly believe that the good faith provisions that Mr. Malcolm and you just discussed, Mr. Chairman, and Senator Bennett discussed, are exactly right. We are not trying to allow companies to hide bad faith actions, but to get companies to the appropriate level of care and trust, we believe this passage of this legislation is essential.

Today, Mr. Chairman, criminals and terrorists are in the driver's seat. The bad actors have great advantages. There are hacker communities out there. They have conventions. They communicate on the Internet. They are not worried about FOIA provisions, but we have to get the good guys together in the same way. We have to get them to cooperate.

One final point. Mr. Dick said quite correctly that the industry and government are trying to work together on a lot of good advances such as the InfraGard program. But we still believe, Mr. Chairman, the government perhaps can do a little bit more to share sensitive information in the other direction. Now, we understand again that is very difficult, and in some industries it is being done, but again, that is trust going the other way. That is the cultural change on both sides that Mr. Tritak referred to, but we would encourage this Committee to continue to dialog with industry and with government to make sure the information sharing is going in both directions.

Thank you very much.

Chairman LIEBERMAN. Thanks, Mr. Miller. Mr. Paller.

TESTIMONY OF ALAN PALLER,[1] DIRECTOR OF RESEARCH, THE SANS INSTITUTE

Mr. PALLER. Thank you, Mr. Chairman.

Every day millions of attacks are launched across the Internet in an ongoing battle between——

Chairman LIEBERMAN. Mr. Paller, excuse me. Tell us what the SANS Institute is.

Mr. PALLER. SANS is the principal education organization in information security. We train about 16,000 people a year, the intrusion detection analysts, the firewall people, the guys on the front lines, and that is who I am representing in this discussion today.

I will start by answering directly the four questions that were outlined in the letter that you sent. The government is not getting the data it needs from the private sector, either to provide adequate early warning or to give a good report to you or to the public about the real costs of cyber crime. On the other hand, specific elements of government are doing a wonderful job of responding very quickly to information the private sector provides. For example, the

[1] The prepared statement of Mr. Paller appears in the Appendix on page 112.

Office of Cyber Security in the White House and the FBI created a wonderful public/private technical partnership to fight specific worms. GSA inside the government is doing a great job of sharing data within the government, getting data reported to it and sharing it within the government. Private sector organizations are not doing very well in sharing attack data. I will give you specific information on that. Although they are making good use of data on unsuccessful attacks, and I will differentiate that in a minute.

The fourth question is whether legislation is needed. I am not a lawyer. I do not have that training, but I believe a clarification of the FOIA exemption is not going to cause companies to share cyber attack data with the government. I fully agree that secrecy of that data is essential when that data is presented, to protect the victim from further damage. You have to keep it secret because if you do not, the bad guys, will pile on. If anybody is known to be attacked, everyone else comes in and goes and gets them, plus you have got all the problems with the business issues.

But even if you provide a perfect FOIA exemption, the companies under attack are unlikely to share the data. There is ample evidence to prove this. Even when the technical trust relationship is established—I think of FOIA as a technical trust. Trust is a personal issue. FOIA is a technical way of trying to build it. Even when the technical trust relationship is perfect, the evidence comes from the members of one of the ISACs, not the oldest ISAC, but the most active old ISAC in this information sharing of cyber data, the Financial Services ISAC. They have a reporting system that is absolutely perfect. They cannot figure out who reported. And so you would think that would solve the problem. But if you go in and check the data, you will find that substantially none of them reported data on current attacks or reported data on other attacks with one single exception, and the exception is actually the reason you think there is data, and that is when they have actually hired the company that runs the ISAC to be their instant response team. So the company that is hired goes in as part of the victim's team, and because they know the data as the victims know it, they feed it into the database. But the idea that if you establish a perfect technical trust relationship, you are going to get the data—we have no proof of that?

Chairman LIEBERMAN. What do you mean by data here?

Mr. PALLER. I mean, "I am being attacked right now. It is coming in through a new vulnerability in IIS. It has gone two steps. It has also taken over my database. They are extorting money from me."

And it is happening right now. Two people get it. One is the consultant that was called in, and if they call the law enforcement in, they will get it, too. But there is no sharing with other people.

Chairman LIEBERMAN. You mean the fact that it is happening?

Mr. PALLER. The fact that it is happening because it is a private event. They are being extorted.

Chairman LIEBERMAN. Understood. So that is what you mean by data here——

Mr. PALLER. Yes, exactly.

Chairman LIEBERMAN. Because they do not want to reveal it. They do not want it to be known——

Mr. PALLER. They do not want to reveal it, and they see no benefit in revealing it.

Chairman LIEBERMAN. And they see danger or vulnerability or loss.

Mr. PALLER. It is a bet-your-company loss. It is that big to them. So all the other stuff tends to pale.

If the government—this is the line they do not like to say, but if the government wants substantially more people to report attack data, I think you are going to need to make reporting mandatory through changes in contract and grant regulations or through other action in legislation like the legislation you have that requires federally insured banks to report suspicious activities.

I have a couple of charts. Is it all right if I show them to you?

Chairman LIEBERMAN. Sure, if you can stay within your time.

Mr. PALLER. Well, since we have 1 minute left, let us not do that.

There are five areas that the data sharing comes in. One is vulnerability data. If a utility finds out it has a vulnerability in a SCAN system, running its systems, it could do a lot of good if it shared that with the government and it could do a lot of good if it shared that with the other utilities right away, and getting that data is absolutely essential to the early warning.

Two, unsuccessful attack date is being shared very well. This is the data that hits your system but you do not want. That data has found two worms and it has helped block one of them and helped capture the criminal that did the other one. So that is working. What is not working are the two sets of data that you want when the attack is taking place, when it is taking place and you are not getting it after the fact, and as I said before, you are not going to get it unless you require it.

The last set of data is the one that actually can do the most good. There is a synthesis of data that companies will share. The synthesis is "we have been attacked, so we know what we have to do to protect our systems," and those are called benchmarks. And when the Federal Government and commercial organizations share the benchmarks, you can actually have a radical impact on the effect of new worms. The NSA, the National Institute of Standards and Technology, SANS and the Center for Internet Security have just finished, with Microsoft's help, standard for securing Windows 2000. There will be more coming shortly. If you want to do a lot of good make sure the Federal Government uses some kinds of standards when they buy new equipment so that they are as safe as they can be when they are installed.

Thank you.

Chairman LIEBERMAN. Thank you. Mr. Sagalow.

TESTIMONY OF TY R. SAGALOW,[1] BOARD MEMBER, FINANCIAL SERVICES ISAC AND CHIEF OPERATING OFFICER, AIG eBUSINESS RISK SOLUTIONS

Mr. SAGALOW. Mr. Chairman, thank you for this opportunity to testify about the importance of information sharing and the protection of this Nation's critical infrastructure.

[1] The prepared statement of Mr. Sagalow with attachments appears in the Appendix on page 123.

My name is Ty R. Sagalow, and I come to you in two capacities today. First as a Member of the Board of the Financial Services Information Sharing and Analysis Center, the FS ISAC. And second, as COO of American International Group's eBusiness Risk Solutions Division, the largest provider of network security insurance in the world. My full remarks have been entered into the record, but I'd like to summarize them for you if I can.

Governor Tom Ridge recently remarked, "Information technology pervades all aspects of our daily lives, of our national lives. Disrupt it, destroy it or shut down the information networks and you shut down America as we know it."

The sad fact is that our information technology systems are already under attack, and there is every reason to believe it will get worse before it gets better. U.S. companies spent $12.3 billion to clean up damages from computer viruses in 2001. And Carnegie Mellon reported that in 2001 they received over 50,000 incident reports. Today it is easier for a cyber terrorist to shut down a dam by hacking into its control and command computer network than to obtain and deliver the tons of explosives needed to blow it up. More frightening, the destruction can be launched from the safety of the terrorist's living room couch, or cave as the case may be.

Fortunately, we are not powerless. Ironically, as it is the information systems which are the subject of the attack, it is our ability to share information which provides our best foundation for defense.

Today the financial institutions that are members of the FS ISAC represent more than 50 percent of all credit assets. The mission of the FS ISAC is straightforward: Through information sharing and analysis provide its members with early notification of computer vulnerabilities, computer attack subject matter expertise and relevant other information such as trending analysis. Unfortunately, I am here today to tell you that we have not been wholly successful in that effort, and we can not succeed without your help.

We believe there are chiefly three obstacles that must be removed for effective information sharing to take place. The reason, as Senator Bennett has already said, companies will not disclose voluntarily if their general counsels tell them that there is a potential that disclosure will bring financial harm to their company. It is really that simple.

As respect to sharing information to the public sector, the fear exists that competitors or terrorists or others will be able to obtain that information through the Freedom of Information Act. As respect to sharing of information within the private sector, there are two fears. First that the sharing will be deemed to be a violation of antitrust laws, as been previously discussed; and second, that the act of sharing the information will lead to civil liability against a company or its directors and officers.

Now, much has already been said of the first two points. Permit to speak on the third for a moment. The chilling effect of the potential liability lawsuits on voluntary speech cannot be underestimated. Private lawsuits, or rather the fear of them, have always played an important role in fostering proper conduct. However, when applied inappropriately, they can have the opposite effect. Such is the situation here. Why disclose the potential inadequacy

of a security technology of your vendors when that disclosure could lead to a defamation lawsuit. Why recommend the use of specific technology safeguards when such disclosures could lead to lawsuits alleging interference with the contractual rights of others? Why freely disclose the result of research and analysis and best practices, when that disclosure could lead to shareholder lawsuits alleging disclosing of company trade secrets?

The risk is too great. Better safe than sorry. Better to keep your mouth shut. These statements represent the danger that we face today as they will be the advice given by general counsels throughout the Nation.

Fortunately, this danger can be avoided through thoughtful and balanced legislation like the Senator Bennett-Kyl bill and similar to the great work done by Senator Bennett in Y2K.

Putting on my other hat for a moment, I can tell you that information sharing is essential to the creation of a stable insurance market for network security. Insurance plays a critical role in protecting our national infrastructure, both through the spreading of risk as well as the influencing of standards of good security behavior through the incentives inherent in making insurance available and affordable.

Today my company leads the way in this effort, and we have already provided billions of dollars of insurance protection for thousands of companies. However, there are very few insurance companies willing to provide network security insurance. The reason, insurance companies cannot underwrite if they do not have access to data on frequency and severity of loss or at least the hope of future access to that data. Effective and robust information sharing becomes the foundation of building the actuarial tables needed to create a stable insurance market.

Therefore and in conclusion, we believe that for voluntary information sharing to be both robust and effective, the following needs to happen: An exemption for FOIA as seated in the Bennett-Kyl bill; an exemption of the Federal-State antitrust laws for information that is voluntarily shared in good faith, and finally, the creation of a reasonable safe harbor provision similar to that that was provided under Y2K, to protect disclosure of information within the private sector as long as that disclosure was made in good faith.

Mr. Chairman, I would very much like to thank the Committee for permitting me to testify on this important subject. I will be pleased to answer any questions you might have.

Chairman LIEBERMAN. Thanks, Mr. Sagalow. Mr. Sobel.

TESTIMONY OF DAVID L. SOBEL,[1] GENERAL COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. SOBEL. Mr. Chairman, thank you for providing me with the opportunity to appear before the Committee.

The Electronic Privacy Information Center, EPIC, has a longstanding interest in computer security policy, emphasizing informed public debate on matters that are of critical importance in today's interconnected world.

[1] The prepared statement of Mr. Sobel appears in the Appendix on page 166.

While my comments will focus primarily on proposals to create a new Freedom of Information Act exemption for information concerning infrastructure protection, I would like to share with the Committee some general observations that I have made as this debate has unfolded over the last few years.

First, there appears to be a consensus that the government is not obtaining enough information from the private sector on cyber security risks. I would add that citizens, the ones who will suffer the direct consequences of infrastructure failures, are also receiving inadequate information on these risks.

There has not yet been a clear vision articulated defining the government's proper role in securing the infrastructure. While there has been a lot of emphasis on finding ways to facilitate the government's receipt of information, it remains unclear just what the government will do with the information it receives. In fact, many in the private sector advocate an approach that would render the government powerless to correct even the most egregious security flaws.

The private sector's lack of progress on security issues appears to be due to a lack of effective incentives. Congress should consider appropriate incentive to spur action, but secrecy and immunity, which some advocate, remove two of the most powerful incentives—openness and liability. Indeed, many security experts believe that disclosure and potential liability are essential components of any effort to encourage remedial action.

Rather than seeking ways to hide information, Congress should consider approaches that would make as much information as possible available to the public consistent with the legitimate interests of the private sector.

As indicated, I would like to focus my comments on proposals to limit public access to information concerning critical infrastructure protection. EPIC and other members of the FOIA requestor community have, for the past several years, voiced concerns about proposals to create a broad new FOIA exemption such as the one contained in S. 1456 for information relating to security flaws and other vulnerabilities in our critical infrastructure. Government activity in this area will be conducted in cooperation with industry, and accordingly, will involve extensive sharing of information between the private sector and government. To facilitate the exchange of information, some have advocated an automatic, wholesale exemption from the FOIA for any cyber security information provided to the government.

Given the broad definitions of exempt information that have been proposed, I believe such an exemption would likely hide from the public essential information about critically important and potentially controversial government activities taken in partnership with the private sector.

Critical infrastructure protection is an issue of concern not just for the government and industry, but also for the public, particularly the local communities in which affected facilities are located.

I believe the proposed exemption is not needed. Established case law makes it clear that existing exemptions contained in the FOIA provide adequate protection against harmful disclosures of the type of information we are discussing. Exemption 4, which covers con-

fidential private sector information, provides extensive protection. As my written statement explains in detail, I believe that exemption 4 extends to virtually all of the critical infrastructure material that properly could be withheld from disclosure.

In light of the substantial protections provided by FOIA Exemption 4 and the case law interpreting it, I believe that any claimed private sector reticence to share important data with the government grows out of, at best, a misperception of current law. The existing protections for confidential private sector information have been cited repeatedly over the past 2 years by those of us who believe that a new exemption is unwarranted. Exemption proponents have not come forward with any response other than the claim that the FOIA provides a "perceived" barrier to information sharing. They have not made any showing that Exemption 4 provides inadequate protection.

Frankly, many in the FOIA requestor community believe that Exemption 4, as judicially construed, shields far too much important data from public disclosure. As such, it is troubling to hear some in the private sector argue for an even greater degree of secrecy for information concerning vulnerabilities in the critical infrastructure. Shrouding this information in absolute secrecy will remove a powerful incentive for remedial action and might actually exacerbate security problems. A blanket exemption for information revealing the existence of potentially dangerous vulnerabilities will protect the negligent as well as the diligent. It is difficult to see how such an approach advances our common goal of ensuring a robust and secure infrastructure.

In summary, overly broad new exemptions could adversely impact the public's right to oversee important and far-reaching government functions and remove incentives for remedial private sector action.

I thank the Committee for considering my views.

Chairman LIEBERMAN. Thanks, Mr. Sobel. And finally, Professor Steinzor.

TESTIMONY OF RENA I. STEINZOR,[1] ACADEMIC FELLOW, NATURAL RESOURCES DEFENSE COUNCIL AND PROFESSOR, UNIVERSITY OF MARYLAND SCHOOL OF LAW

Ms. STEINZOR. Mr. Chairman, thank you for the opportunity to appear before you today on behalf of the Natural Resources Defense Council.

The issues before you are both significant and troubling, especially in the wake of the tragedies that began on September 11. Obviously, all Americans recognize the importance of doing whatever we can to improve homeland security. At the same time, as Senator Lieberman said, this country was attacked because we are the most successful democracy the world has ever known. If we overreact to those who attacked us so viciously, and in the process undermine the principles and rule of law that have made us such a hopeful example for the world, terrorists will win the victory that has thus far eluded them.

[1] The prepared statement of Ms. Steinzor with an attachment appears in the Appendix on page 172.

NRDC strongly opposes both the text and the underlying principles embodied in S. 1456, the Critical Infrastructure Information Act, and urges you to consider more effective alternatives to make Americans secure.

We oppose the legislation for four reasons. The legislation has an impossibly broad scope. To the extent that the legislation focuses on cyber systems, and by these I mean systems that are connected to the Internet and therefore are vulnerable to outside disruption, NRDC as an institution has little to add to the debate. Computers are not our area of expertise. In fact some of us are still using the Windows 95 operating system.

Of course, as Senator Thompson has articulated, S. 1456 extends much further than cyber systems, covering not just computers that are connected to the Internet, but also the physical infrastructure used to house these systems. The legislation covers not just physical infrastructure that has or is controlled by computers, but also any physical infrastructure that is essential to the economy and might be damaged by a physical attack. The legislation is not limited to the Freedom of Information Act, but extends to any use by anyone of the information in civil actions. Mr. Malcolm spoke about the government's use of disinformation. I would stress, however, that this applies not just to the government but to the use of the information in a civil action by any party.

And the legislation covers information, not just copies of specific documents. It is a slender reed to rest on the adjective direct use when it covers information so broadly, and information in a different format could still be precluded from use in a civil action.

NRDC is sensitive to the fears all Americans have about our vulnerability to terrorist attacks. We are active participants in the debate about whether information about the operation of facilities during acutely toxic chemicals should be accessible on the Internet. The Environmental Protection Agency is encountering many challenges as it works diligently to sort through these issues.

But these difficult issues are not within the areas of expertise of the government agencies assigned a role in implementing S. 1456. Using legislation of this kind as a vehicle for stressing how information enhances or combats the terrorist threat to physical infrastructure is unwise and duplicative. As Senator Akaka stated so well, the legislation will have a series of disastrous unintended consequences, damaging existing statutory frameworks crafted with care over several decades.

Let me draw in another thread of history. A few years ago major industry trade associations, which had members subject to environmental regulations, began to push the idea of giving companies immunity from liability of the performed self-audits, uncovered violations of the law, took steps to solve those problems and turned the self-audit over to the government voluntarily. The Department of Justice vigorously opposed such proposals and they never made it through Congress. Several States enacted versions of self-audit laws. In the most extreme cases, EPA responded by threatening to withdraw their authority to implement environmental programs and the laws were repealed.

Self-audit bills defeat deterrence-based enforcement, creating a situation where amnesty is available even where a company has

continued in violation for many years and then decided to come into compliance at the 11th hour.

As drafted, S. 1456 is a comprehensive self-audit bill that extends not just to environmental violations but to violations of the Nation's tax, civil rights, health and safety, truth-in-lending, fraud, environmental, and virtually every other civil statute with the exception of the Securities Act. The legislation does not even require that companies cure their violations in order to receive amnesty. Redrafting may help, but it will be very hard to solve the problems as long as the legislation covers physical infrastructure. Secrecy is not the best way to protect critical infrastructure, and this Committee should abandon that approach. Rather, actually requiring changes on the ground is a far preferable solution to the threats we face.

One way to reduce the vulnerability of physical infrastructure is to ensure that employees have undergone background checks and that site security at the fence line of the facility and the area adjacent to vulnerable infrastructure is enhanced.

Another way to protect the public and workers is to eliminate the need for the hazardous infrastructure, for example, a tank holding acutely toxic chemicals. This approach, called Inherently Safer Technologies, is the cornerstone of legislation, S. 1602, now under consideration by the Senate Environment and Public Works Committee.

NRDC has also consulted with EPA officials responsible for coordinating their agency's contribution to strengthen homeland security. EPA has extensive legal authority to take actions against companies that fail to exercise due diligence in protecting such attacks. The combination of the Corzine bill and administrative action will make great strides toward addressing these problems.

As the Committee continues its consideration of these issues, we hope that you will continue to consult with a broad range of experts and stakeholders and allow us to participate in your deliberations. We appreciate the efforts of the Committee staff to undertake these discussions in order for all of us to better understand the policies, goals and implications of the legislation. Thank you.

Chairman LIEBERMAN. Thanks, Professor.

Let me see if I can ask a few of you to give a little more detail, without disclosing exactly what you do not want to disclose, which is what are we talking about here with sensitive information? Mr. Paller, in your testimony you gave us a series of examples. I wonder if any of the rest of you, Mr. Sagalow or Mr. Gent, could give us a little more general information about what we are talking about that people you represent or you yourselves would not want to disclose without this kind of exemption from FOIA?

Mr. GENT. Senator, you might remember back, I believe it was your freshmen year this Committee held hearings, and not much has changed about the electric system vulnerability since then. And one of the problems back then was that they wanted us to build a list of critical facilities, "they" being the government, so that the government could analyze that and be prepared to help us defend at those facilities at that time from physical attack of nations or nation states or terrorists. Not much has changed. We now have the cyber element that goes into this.

So government agencies are asking us to come forth with lists of critical facilities along with their degree of vulnerability and what would happen if this facility were taken out. And we have, for the last 20 years, said that we are not going to build such a list. As others have testified, we have no confidence that the government can keep that a secret.

Chairman LIEBERMAN. Got it. Mr. Miller, do you have an example that comes to mind, generally speaking?

Mr. MILLER. In the information technology industry there might be a product that is developed, a software product, which in most formats works fine, but in conjunction with a certain hardware, which a lot of these things are integrated with, different types of hardware, in fact there is a vulnerability. The software vendor may become aware of that, may decide that it wants to communicate with, however, a very limited audience, for example—just its immediate customers and clients because of that relationship, but would be totally unwilling to share that with the government because it does not want to face the possibility of broad public disclosure of that.

Again, we are talking about limited cases, not a massive virus attack, where as was discussed in the previous panel, everyone wants to work together to get the word out about a Code Red or a Nimda. We are talking about a particular—the technical term is "configuration" of a particular software product, where the impetus is to keep it in a closed community unless otherwise they are incented to do so, and particularly to share it with the government would bring a lot of risk because of this possibility, or Senator Bennett, maybe it is just the paranoia business, the likelihood that if you share it with government it will end up being disclosed.

Chairman LIEBERMAN. Mr. Sagalow.

Mr. SAGALOW. Mr. Chairman, I will give you two examples of information, falling into the areas of best practices that might be shared if there was a FOIA exemption. When it comes to the Nimda virus, Code Red, those massive attacks, that information is being shared. What is not being shared is information on risk management techniques, best practices, corporate governance, and I will give you two examples.

If a corporation becomes dissatisfied with their particular vendor, one antitrust software works very poorly and they end up deciding to terminate that contract and instead incorporate another antivirus software, you would want that information to be shared. A general counsel would be extremely reluctant to give their CEO or CTO permission to share that type of information, fearing potential defamation lawsuits from the vendor that you ended up dropping, as well as from other people for other causes of action like tortious interference with a contractual relationship.

The second example I would give you is potential shareholder actions arising out of disclosure of company practices and technology use. There is a business issue of whether you want to disclose these things since some may regard them as trade secrets. However, if all the CEOs of the world were similar to Mr. Bennett, they would disclose a certain amount of what is arguably a trade secret if it is consistent with protecting our national infrastructure and the good of society, as long as it did not do undue harm to the com-

pany. A general counsel is not going to take that attitude. A general counsel is going to say even though it is the right thing to do, there are professional plaintiff attorneys out there that will start shareholder derivative actions alleging that the act of disclosure itself was a breach of fiduciary duty.

Chairman LIEBERMAN. Thank you.

Mr. Paller made a statement which was very frank and sounded pretty realistic, that even with the exemption proposed, that there will be companies who will not share because they are still concerned in a voluntary system that it will not really be kept confidential, and therefore—not that he was recommending this, maybe he was—but that we may need a mandatory system.

Now, I wonder whether, real quickly because I want to get on to another question, whether the three of you agree or disagree, if we had appropriate exemption from FOIA do you think companies would still withhold information?

Mr. GENT. I think if you made it mandatory, they would not withhold.

Chairman LIEBERMAN. Right. [Laughter.]

Mr. MILLER. I would strongly disagree with Mr. Paller. First of all, I do not know what it would mean to be mandatory and I do not know how you would possibly enforce that, but I think the information sharing is growing. Again, I agree that the FOIA is not the silver bullet, Senator, but for the interest of the industry, yes, there is growing in the communities, electrical, financial services IT, that there is a broader community interest because these people who are American citizens. They want to support the good of the Nation. But they have to be protected on the down side. That is clearly the establishment of the ISACs, the establishment of the partnerships, that sharing of information through InfraGard is a commitment the industry is making.

Chairman LIEBERMAN. Mr. Sagalow.

Mr. SAGALOW. Our members have told us that if these obstacles are removed, there will be a substantial increase in disclosure. Of course some people will never disclose no matter what, but there will be a substantial increase.

Chairman LIEBERMAN. Professor Steinzor, let me ask you your reaction to the conversation on the last panel, which was: Why would not your concerns about the effect of the passage of Senator Bennett's legislation on various environmental laws be eliminated by inserting language that said that nothing in this proposal should diminish any obligation that anyone has under any other system of law?

Ms. STEINZOR. That would go a long way to help, but we would still be required to fight over such issues as whether there was an obligation, there was no obligation, and whether the information was submitted before the government asked for it. The way this bill is drafted it says that information is voluntarily submitted in the absence of such agency's exercise of legal authority. So the agency would have to actually ask for the information in order for it to be submitted non-voluntarily. At the moment, there is a lot of information kept in companies that the government may not have asked for yet, and if it was submitted voluntarily, the protec-

tion could be asserted. That is just one of the kinds of problems that we are concerned about.

Another way to deal with what you are talking about is a savings clause. Such a clause should be something that is dynamic, not just for laws that are on the books today but laws that are added to the books in the future.

And one last thing I would like to add, which is that to the extent that the information we are concerned about here is information that is time-sensitive, one way to approach it would be to say the protection only lasts for a certain limited period of time. We have heard a lot about an attack is ongoing and you need to share the information. Arguably, once you have shared it, once the problem is addressed, as we all assume it will be, you no longer need to make that information secret. Keeping it secret is only important to liability down the line. Again, there would be no liability if the problem was solved. So that is another way to approach this.

Chairman LIEBERMAN. Mr. Sobel, do you have a reaction to that discussion on the first panel? I know is it not directly responsive to your concerns.

Mr. SOBEL. Frankly, Senator, my concern is with this taken in combination, the fact that there would be no possibility of disclosure apparently at any time running into the future, as well as no real governmental ability to address any of the vulnerabilities that are made known to the government, and then there is this provision that I read as a very broad immunity that would also preclude any private actors from seeking corrective action. So what I see, taken as a whole, is this structure that provides information to the government, but then really ties the hands of the government or anyone else to direct and compel corrective action. As I said, I think this approach protects the negligent as well as the diligent, and that is really, I think, the main flaw. Yes, we can certainly assume that many, if not most, of the actors in the private sector are going to be good actors, but it seems to me that this just creates an incredibly large loophole for those companies that frankly are more inclined to be negligent than diligent.

Chairman LIEBERMAN. Thanks. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman, and thanks to everyone on the panel including those who were not quite as supportive of my legislation as some of the others, because these are obviously the issues that have to be resolved, that have to be talked about.

I sponsored a bill for a long time on the privacy of medical records, and ran into much the same kind of very firm opinions on all sides of the issue, and I kept saying year after year, this is not an ideological issue, this is not conservatives versus liberals or Republicans versus Democrats. This is a management issue. How do we solve the problem? And my staff got sick and tired of me saying it. I would say, if there is a management problem raised by this objection, let us solve the problem rather than put ourselves into ideological camps and then scream at each other? We do a great deal of that in the U.S. Senate, usually on the floor, less so in committee, but we have a serious challenge here. It is one for which there is, frankly, no historic predicate because the coming of the information age has changed the world as thoroughly and fundamen-

tally as the coming of the Industrial Age did. And if you are going to talk about agricultural age warfare after the invention of the repeating rifle, you are going to be left behind. And the statement by Osama bin Laden is a chilling reminder of the fact that we live in an entirely different world, and we all, on all sides of this issue, need to view that world differently.

Now, if I were someone who wished this country ill, and I have said this before so I am not giving out any secrets, if I were someone who wished this country ill, I would be concentrating on breaking into the telecommunications infrastructure over which the Fedwire functions. If I could shut down the Fedwire, I could bring all activity in the country to a complete stop. No checks would clear. No financial transactions would take place. There could be no clearing at the end of every day for the Federal Reserve system. The Fedwire is the absolute backbone of everything that goes on in the economy. And I have had conversations with Chairman Greenspan about protecting the Fedwire from cyber attack. That specter before us, how do we deal with the challenge of telephone companies, of power companies, of brokerage houses, banks, and the Federal Government itself, that are tied together in this absolutely intricate network of transactions and facilities, and protect the Fedwire from someone sitting in a cave somewhere coming after it?

Now, Mr. Miller could share some information with us, which I have seen, that shows the graphs of the level of attacks that have come against the United States, cyber attacks, and it is a logarithmic scale. It is not just a quiet little incremental increase every year. It is almost Malthusian in terms of the predictions, and it is a hockey stick. And I have stood in the rooms where these attacks are being monitored in real time, second by second, in the Defense Department within the Pentagon. The interesting things is that just as the number of attacks is going up logarithmically, the sophistication of the attacks is going up logarithmically, so that our ability to defend ourselves, which is also going up logarithmically, is just barely keeping up with the sophistication and volume of the challenge that we have.

I first became aware of this with Y2K when I was talking with Dr. Hamre, the Deputy Secretary of Defense, as we were trying to find out in a hearing on S. 407, Mr. Chairman, over in the Capitol, where we can have classified briefings, about the degree of this country's vulnerability, and Dr. Hamre said to me, "We are under attack every day." And this was 3 or 4 years ago. And I said, "Under attack, what are you talking about?"

Well, the attack on the government facilities goes on. My fear, the thing that keeps me awake at night is that if those who are mounting those sophisticated attacks on government facilities—and they are primarily aimed at the Defense Department and the intelligence community, CIA, NSA and others—were to shift their focus onto the private sector and do so in a timing and a circumstance where no one in the government knew that that shift had taken place, how vulnerable are we, and how will we feel if we say, "Well, we did not facilitate the opportunity for people who are the recipients of those attacks to share with the government what was happening." This is not questioning. I am just responding to the panel

and sharing with you my deep, and I hope not paranoid, desire to see to it that we are prepared for this.

So in the one minute left before we go back to the second round, do any of you, recognizing this is a management issue rather than an ideological issue, have any comments across the gap that has occurred within the panel, that are not just, oh, you are wrong, you do not understand. It is easy for you to say that back and forth to each other. Do any of you have any solutions that you could suggest across the divide that has been created here within this panel in the circumstance that I have framed?

Mr. MILLER. Just a brief comment. I thought that Mr. Sobel and Professor Steinzor said that with some of the limitations that Chairman Lieberman suggested, and Mr. Malcolm discussed it in the earlier panel with you as the primary sponsor, that they might see some possibility of bridging the gap. Again, these are technical legal issues beyond my exact area of expertise, but I was pleased to hear that both Mr. Sobel and Professor Steinzor indicated that they might—if the language of the bill was even more clear as not to allow the worst bad actors to use the Freedom of Information Act language to hide behind—that they might be open to some kind of compromise. And I thought that was a very positive statement by both of them from my perspective.

Ms. STEINZOR. Senator, I could not agree with you more that this is an enormous challenge and a grave threat, and I am not by any stretch of the imagination questioning your motives or your sense of urgency about all of this. What is troubling to us is that it would seem as if a more direct way to approach this would be to try and develop technologies like the one Mr. Paller was talking about, to erect firewalls and make cyber systems more secure, rather than simply allowing for a shroud of secrecy to go over them because of the difficulties of drawing lines in this area.

You know the Freedom of Information Act, in our experience, is one of the most ponderous legal tools one can ever use. It takes months, years, to get a request answered. And so we are puzzled why the urgent exchange of information could not be protected in a short timeframe in a different way that does not implicate the Freedom of Information Act, which we do not see as a very grave threat to the immediate exchange of information. People are talking about perceptions on all sides, and we are puzzled by that.

Mr. SOBEL. Senator, if I could just follow up on that, on the FOIA point. I have a real concern that a new exemption approach could actually muddy the waters far more than they are right now. We have heard a lot of concern about the advice that a general counsel might give within a company in terms of whether or not there is adequate protection or not. It seems to me, as an attorney who looks at these issues, that 28 years worth of very clear case law would give me much more comfort in advising a client than a newly-enacted piece of legislation that contains some very broad language. I think if I was that general counsel and this legislation passed, I would say, "Well, you know, this has not yet been judicially construed. We do not know how much protection this is going to provide." I would feel much more comfortable looking at the Critical Mass decision from the D.C. Circuit, where the Supreme

Court denied certiorari, and saying, "This is a pretty good assurance that this information is not going to be disclosed."

So I do not think we are disagreeing about goals, but I think there is a real question in terms of what is the most effective way of providing the assurance that the private sector seems to want.

Mr. MILLER. Maybe that is what the hypothetical general counsel would believe, Senator Bennett. That is not what the real general counsels believe.

Mr. SAGALOW. Senator, let me follow up if I can.

Chairman LIEBERMAN. Mr. Sagalow, let me just interrupt.

Senator Bennett, I do not have any other questions. I have a couple of colleagues waiting to see me. If you are able, I would like to ask you to continue the discussion, and then when you are through, to adjourn the hearing.

Senator BENNETT. That is very dangerous on your part. [Laughter.]

Chairman LIEBERMAN. I do not want you to get comfortable with the gavel though. [Laughter.]

Senator BENNETT. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Not at all. Thank you for your leadership. It has been a very interesting, important, constructive hearing, and I look forward to continuing to work with you, Senator Bennett, and with those who have been before us to see if we can resolve this in the public interest. Thank you.

Senator BENNETT [presiding]. Thank you very much.

Now, having no constraints upon me, I would like to pursue this a little further.

Mr. SAGALOW. Senator, if I could just respond to a couple of the comments that were mentioned earlier. My company created something called a Technology Alliance, which is a group of technology companies that advise us as underwriters on evaluating cyber risk, and we have been literally talking to dozens of technology companies over the last 2 years and we continue to talk to them.

I can tell you, Senator, that without exception there is no technology company that believes that there is a technology silver bullet. There is no super firewall. There is no super anti-virus or intrusion detection system. There is no single technology or combination of technologies that will solve this problem.

On the second issue of the theoretical versus practical general counsel, I agree with the comments of my colleague, Mr. Miller. I do not know what theoretical general counsels say, but I know what they say to me every day. And what they say to me every day is their view of current law and regulation including case law does not give them a sufficient basis to recommend to their CEOs to disclose. More legislation, more action is needed.

Senator BENNETT. Let me follow through on that one.

We have always been under the impression that we were helping FOIA by focusing and defining the exemption which, Mr. Sobel, you indicated has been done by case law so as to make it clear that in this circumstance under these conditions the broad exemption that is already in FOIA would clearly apply and that we were not in any way repealing or destroying FOIA, we were simply focusing the definition.

Now, Mr. Sagalow, let us go back to you—recognizing you have not had this discussion, but your perception of how a general counsel would react. Do you think that the passage of this legislation would be viewed in that regard and therefore make a general counsel more likely to say let us go ahead, or do you think they would react to the legislation somewhat in the way that Mr. Sobel is? You do not have to agree with his opinion of where they are in case law, as to try to say maybe he is right that they would say, "Well, the legislation may sound good, but it is still not going to give me any comfort."

Mr. SAGALOW. I do not know. It is a legitimate issue. I believe that, based upon the conversations that I have had so far, that the majority of general counsels would be looking at it in the first approach. They would be looking at this legislation clarifying existing case law in a way favorable toward disclosure as opposed to a de novo aspect of legislation that they would feel uncomfortable with until years of case law interpretation.

Senator BENNETT. Let us go back to Professor Steinzor's comment about time. I think that is a very legitimate issue that she has raised. I have used the example which, frankly, Professor, you shoot down, that Osama bin Laden would mount an attack and then file a FOIA request to find out how well it worked, and if indeed FOIA would require 4 years before he got the information, the technology would have been about five generations old by the time he got the information.

She has raised an interesting question, gentlemen, about putting a time limit on this, where you say the FOIA request cannot be filed for 3 years, let us say, pick a number. She would probably pick 3 months, but let us pick a number and put a timeframe on this, and talk about what effect that might have in the real world. Mr. Gent.

Mr. GENT. Senator Bennett, there are certain operational information that can be made availble moments afterwards, some hours afterwards, some days afterwards, but when it comes down to the configuration and vulnerability of the electric system, this is something that evolves over decades. So having information, in fact, to be honest with you, some of the information that is now being released to the public is still very dangerous and could be considered as a terrorist handbook. So the configuration has not changed that much. The components that are vulnerable have not changed that much over the last decade. So if you talk about operational information, I would be willing to talk about a shorter timeframe, but physical configuration of a system is still important after decades.

Senator BENNETT. We need to remember, and you have reminded us, that the physical and the cyber are inextricably linked here.

Mr. GENT. We believe that. In fact, Hoover Dam is not going anywhere.

Senator BENNETT. But the ability to break into the computers that are updated that control the sluice gates, somebody could open the sluice gates and drain Hoover Dam without blowing it up. Is that an accurate——

Ms. STEINZOR. But, Senator, that again is a cyber issue which presumably would be addressed by technology evolving within a certain period of time because cyber systems are changing all the

time. I think the emphasis on the physical configuration is exactly what concerns us because a lot of the physical configuration, for example, at a chemical plant, is heavily scrutinized and regulated by the government. And again, this protection does not just apply to Freedom of Information Act, it always applies to use in a civil action which could be either enforcement or some other type of action that would not be able to proceed if the company was not continuing to do something wrong.

So again, my suggestion about the temporal aspect is that the assumption must be that once we discover vulnerability, we are going to address it right away, whether it is in the physical context or the cyber context, that the Freedom of Information Act in civil actions would only be viable if those problems were not addressed, and therefore a temporal limitation might be just the ticket to solve the problem.

If I could just add one more thing. As an educator of young lawyers, let me talk about the theoretical versus the actual general counsel. One of the things we always impress on our students is the need to zealously protect their clients' interests, and while I would sign up tomorrow to be your general counsel, you being the hypothetical CEO——

Senator BENNETT. You might not be in a financially successful institution. [Laughter.]

Ms. STEINZOR. Well, but you were articulating such good ethics and good sense, that I think I might do it. Maybe I could keep my university job.

The problem is that if there is an opportunity to do a document dump, which of course would not be conceived in those pejorative terms, that it is both a theoretical and actual general counsel would be pushing the company to do exactly that. They would say, "Look, CEO, we have vulnerabilities involing our physical infrastructure that are very serious, and we should go contact Governor Ridge about those and get into some conversation with him, and if any agency tries to pursue us through one of the more mundane daily laws, we can fend them off while we address our vulnerabilities." This kind of situation is our concern.

I should have brought a lawyer joke for the occasion.

Senator BENNETT. I have plenty of those.

Ms. STEINZOR. Good.

Senator BENNETT. Anyone want to respond to that? Mr. Miller.

Mr. MILLER. Not so much to that, but your earlier question about time limitations. It is easy for me to say sure, why not in the information technology industry because 3 years is an eternity. But again, it is very much tied to physical issues.

A certain governor of a certain large State just to the north of here, about 4 years ago was very proud to release a document on the Internet that showed where every telecommunications, electrical network, and critical asset in the Commonwealth of his State was located, and it was very public, it was very well known. I am sure Tom Ridge was very proud of that at the time he was governor, because everyone was into disclosure using the Internet. I am sure looking back from his current position, Tom Ridge wonders how he had that crazy idea 4 years ago to make that information public.

So I would think, Senator, we need to consult with a lot more people who are, as Mr. Gent was suggesting, involved in these long-term fixed positions that may or may not be controlled by cyber relationships before we would say that the time limit idea intrinsically is a good idea.

Again, in principle, I do not think the IT industry would be too much concerned about that, but I think a lot of our customers might be because those physical assets do not change and those physical vulnerabilities do not change for long periods of time.

Senator BENNETT. Without treading into classified territory, because in this whole process I have spent an awful lot of time in places that deny that they exist after I leave them, as a general principle, someone who is looking over critical infrastructure needs to know key points. And the key point in the critical infrastructure can be taken out with a kinetic weapon many times more efficiently than it can be taken out with a cyber attack. The interesting thing that comes from those who analyze this—and I must be careful about this—the interesting thing that comes from those who analyze this for a living is that the key points in a critical infrastructure are very often not obvious. There might be a particular switch in a particular pipeline or a particular telecommunications switch, or a substation that for some reason is far more critical than any other in terms of possibly shutting down the power grid. A terrorist would give a tremendous amount to know where those key points are. And I am not sure the people who are giving information to the government, if my bill was to pass, would themselves know how key they are or where they are.

And the question becomes—the government could put that together. The government says, "OK, we have got this from this source. We have got this from this source. Uh-oh." Back to my original analysis if I am going to mix metaphors here. If this particular facility goes down, that is what shuts down the Fedwire. And the people who manage that facility do not know that. If that information—that is the pieces of information that allowed the government to discover that are individually made available with FOIA, and an analyst working for a hostile nation state comes to the same conclusion that our analyst came to, and said, "Aha, this is the one thing which if we shoot down, cuts down the Fedwire." And that become very valuable information, and maybe they make the decision, "We are not going to go after it in a cyber way. We are going to get somebody with a truck full of fertilizer to pull up to the front door of that particular facility and lo and behold everybody is going to be surprised because they think they have all of these technological firewalls everywhere else to protect the Fedwire, and bingo, we can take it out with a fertilizer bomb."

Now, that is obviously a hypothetical and obviously that kind of analysis is going on. But that is the kind of concern that I have about sharing information. And it may well be that we could find a division here between some things that could be disclosed after a 3-year period and some things that could not. I can anticipate some of you are going to say, "Well, you are not going to know that in advance," but let us at least have a quick round on that concern.

Mr. PALLER. I think you go back to the bigger question that your staff got mad at you about, about understanding it is a manage-

ment problem. And what I see happening here is what happens in lots of security conversations, which is different people looking at different parts of the animal. (1) If that is what you are going to disclose, it is terrible, and (2) if that (other thing) is what you are going to disclose, it is fine. I think maybe this is one of those really hard slogging jobs where you have to go systematically through every specific type of data in every specific type of environment and get the answers to the questions of which are going to be disclosed and which are not going to be disclosed if you want to get consensus in the room. I am not sure that the effort is going to be worth the trouble, but I do not see a way, as long as you keep a very broad view of what the "it" is, to get them to agree how long or when or whether to disclose it.

Mr. MILLER. Senator, I do not know whether it has to do directly with FOIA legislation. I mean clearly the issue of saying we do not know what we do not know is a real problem. Let me give you an obvious lesson that was learned on September 11, and that is redundancy in telecommunication systems. A lot of companies had learned over time, as part of business continuity planning, to have redundancy in their telecommunication systems, which meant having two carriers, two switches, and two sets of pipes. But a lot of companies put those switches and those pipes in exactly the same building, the World Trade Center. So when the World Trade Center went down they really did not have redundancy. They ended up not having complete telecommunication systems left. And so that was a lesson that was learned, or at least it was put out there. I am not sure whether it has been completedly learned. We are still having this debate with the Federal Government as you know, and there is legislation in Congress to require Federal agencies to begin to think about having true physical redundancy as opposed to assumed physical redundancy in telecommunication systems.

So frequently we do not know what we do not know, and we have to have a tragedy or a direct experience to learn that lesson.

Would the FOIA exemption you are suggesting help that to come together? Perhaps because who, other than the government, does exactly what you say, which is to look at all of the pieces of the puzzle. At the end of the day, his companies look at the electricity industry, I look at the IT industry, Mr. Sagalow and financial ISAC members look at the ISAC industry. Mr. Paller kind of looks across industries because he has got experts in all of these. But at the end of the day it is only the government that looks at the overall view of how these interdependencies really work in ways that nobody else really can.

Mr. SOBEL. Senator, I just wanted to make the observation that it seems to me that there is a little bit of a disconnect in terms of industry's attitude here. I mean on the one hand we are being told that the agencies that would receive the information are somehow so incompetent that they would be releasing highly sensitive information in response to a FOIA request despite very strong case law supporting withholding, and yet on the other hand industry seems to believe that there is something valuable that the government has to tell them or something valuable the government has to do in the form of coordinating response activity. So I am not getting a clear picture from industry in terms of how they see government.

Is government a competent, useful player here or is it something else, an entity that is going to receive information and very haphazardly release it to the detriment of all of us?

So I really am hearing two things here.

Senator BENNETT. My answer to that question would be yes. [Laughter.]

Mr. SOBEL. Well, then I think it raises——

Senator BENNETT. There is no such thing as industry and there is no such thing as the government. There are a variety of companies in a variety of industries. It is enormously complex, and as you have indicated, the vast majority of them would be very disciplined and act in a responsible way. And there are few, in your opinion, that would not, that would be irresponsible and would try to use this in an improper fashion. There are a variety of people in government who are enormously competent and who would provide the analysis that we need, and there are a variety of people who have demonstrated a regulatory mentality to which I referred earlier, that would use the information in a way just to prove their regulatory muscle that would be irresponsible. You only have to sit in a Senator's office to discover that there is no, "the Government." There are a variety of human beings, some of whom, most of whom, act responsibly and intelligently, and every once in a while there are some regulators who just defy common sense in the way they do their jobs and hang on to the regulations that they have.

So my answer to your question, without being facetious, is yes to both sides of it.

Mr. SOBEL. I think that is very true, but as Mr. Tritak said, if this is a question of trust and establishing trust, I do not understand why that same regulator is suddenly going to be trusted by the industry submitter to comply with your new FOIA exemption if he is not trusted to comply with the existing protections. In other words, if this is an incompetent or malicious bureaucrat, why would this new legislation create any greater trust on the part of the submitter? That is what I am really missing here.

Senator BENNETT. All you can hope for is that you nudge him in the right way.

Mr. SAGALOW. Senator, if I could just emphasize on that last point you mentioned, because that is exactly what is happening. In the real world everything is a gray area and what you need to do is nudge the general counsel in the right way. What I am hoping that you are hearing from at least the majority of people that are speaking on this area is a desire not to throw the baby out with the bath water, that this is a very essential piece of legislation, very important to the national infrastructure and our war against terrorism, and that the people on both sides of the aisle, so to speak, are willing to look at language in the bill consistent with the fundamentals: That data is received through independent use would be exempted, that under certain circumstances criminal prosecution if documented through that independent use would be permitted, that certainly it is not the intention of the legislation, and none of my members are indicating they expect it to be the intention of the legislation, that the legislation will somehow allow a company not to disclose what they would otherwise be obligated

to disclose, whether in the criminal area, the environmental area, or the financial area.

Two other quick comments. My personal belief is that the fear of data dumping or the bad general counsel while not unrealistic, is perhaps overstated. General counsels have a firm belief in the law of unintended consequences. That is why they are hesitating to permit disclosure in the first place. And part of the law of unintended consequences is if you do a data dump thinking that you are going to fool the other side, something is going to go wrong. Very few general counsels take that risk unless it is a matter of utter desperation.

And then finally on this issue of the temporal solution to the problem, I can only echo the point that was made earlier, that this issue of "we do not know what we do not know" is quite important. We really do not know in any set of documents or data what are the fundamental issues that may be completely applicable 5, 6, or 10 years from now.

Senator BENNETT. Well, the audience is voting with their feet in saying that the hearing is over. May I thank all of you for your contribution. This has been a serious discussion rather than a simple venting of opinions, and I am grateful to all of you for your willingness to enter into it in that spirit.

If I were to summarize my attitude, and speaking solely for myself, obviously, and not for any other Member of the Committee, I wish we had the time to go through all of the issues and ultimately come, as has been suggested here, to a final consensus where everybody buys off and agrees, because I think people of goodwill at all aspects of this probably could arrive there.

I must share with you once again, I feel a sense of urgency here which is very powerful, and the more time I spend with the intelligence community, the more time I spend in the Defense Department, the more times I visit that room in the Pentagon, where the attacks on our military infrastructure come in in real time and I see them on the screen, the more sense of urgency I have.

I think we err on the side of exposing our country and really with exposing the American economy, exposing the world to serious damage if we delay too long. And I would rather take steps as quickly as we can that start us down the road and maintain a perfect willingness to change the legislation as we get examples of serious violations of environmental or other circumstances by the small minority of companies that might try to take advantage of that, than delay the legislation until we can theoretically iron out all of the problems.

I do not wish to be an alarmist. I try not to be an alarmist, but I think this is an issue that requires early action. And that is why I am grateful to the Chairman for his willingness to schedule the hearing, and I am grateful to all of you for your willingness to participate.

With that, the hearing is adjourned.

[Whereupon, at 12:30 p.m., the Committee was adjourned.]

APPENDIX

PREPARED STATEMENT OF SENATOR BUNNING

Thank you, Mr. Chairman.

During the past 7 months community leaders, government officials and average Americans have been re-evaluating the level of security needed to protect ourselves.

We have seen dramatic changes in the airline industry, and we have become very concerned about the safety of our ports and other transportation systems.

Local, State and Federal emergency personnel have been on a high state of alert. And, we are increasing staffing at our borders. However, protecting our critical infrastructure is one of the most important steps we can take to ensure a safe future, and it should not be overlooked.

The government needs to do everything it can to encourage companies to share information with each other and Federal officials in an effort to stop those who are attacking our country.

I understand that some companies are concerned about sharing sensitive information because they are afraid it may be released to the public.

If we are serious about protecting our critical infrastructure, then we have got to be serious about finding a solution to this problem.

If businesses are afraid their non-public information can make its way into the public domain, we will never get the kind of open and productive relationship that we need between the government and business community.

I am looking forward to hearing more about the legislation introduced by Senators Bennett and Kyl that begins to address this problem, and I appreciate the time our witnesses have taken to testify today.

Thank you.

Statement for the Record of Ronald L. Dick,
Director, National Infrastructure Protection Center
Federal Bureau of Investigation
Before the
Senate Committee on Governmental Affairs

May 8, 2002

Mr. Chairman, Ranking Member Thompson, and members of the committee, thank you for inviting me here today to testify on the topic, "Critical Infrastructure Information Sharing." Holding this hearing demonstrates your individual commitment to improving the security of our Nation's critical infrastructures and this committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. We have seen how a terrorist attack can have immediate simultaneous impact on several interdependent infrastructures. My testimony today will address information sharing as it relates to our mission at the National Infrastructure Protection Center. Our combined mission supports information and physical security, law enforcement, national security, and the military.

As set forth in Presidential Decision Directive 63 (PDD-63), the mission of the NIPC is to provide "a national focal point for gathering information on threats to the infrastructures" and to provide "the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." The Directive defines critical infrastructures to include "those physical and cyber-based systems essential to the minimum operations of the economy and government," to include, without limitation, "telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." To accomplish this mission, we have had to build a coalition of trust, one . . . amongst all government agencies, two . . . between the government and the private sector, three . . . amongst the different business interests within the private sector itself, and four . . . in concert with the greater international community. Once trust has been earned, true two-way information sharing can occur. The NIPC shares information across the public and private sectors through several programs and mechanisms, with a focus on cyber security.

SHARING INFORMATION WITH FEDERAL AGENCIES, STATE AND LOCAL LAW ENFORCEMENT AUTHORITIES, THE PRIVATE SECTOR, AND INTERNATIONALLY

OVERALL NIPC INFORMATION SHARING EFFORTS

The NIPC routinely shares information with the public and private sectors to help them better protect themselves. That does not mean that information is broadcast across the news media in every instance. While public statements are the best alternative in some cases, in other cases the NIPC has approached victim companies or government agencies privately. In many

cases a tiered approach is taken so that information with the appropriate level of detail reaches the right audiences. If the NIPC finds that despite issuing an advisory, a widespread problem persists or grows, then an advisory may be reissued.

The NIPC has a variety of information products to inform the private sector and other domestic and foreign government agencies of the threat, including: assessments, advisories and alerts; a *Daily Report*; biweekly *CyberNotes*; monthly *Highlights*; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, *Highlights* is a monthly publication for sharing analysis and information on critical infrastructure issues. It provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in an unclassified format and reaches national security and civilian government agency officials as well as infrastructure owners. *CyberNotes* is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published twice a month on the NIPC website (www.nipc.gov) and disseminated via e-mail to government and private sector recipients. Although the NIPC can and does issue limited distribution products that are classified or law enforcement sensitive (for example, because they reflect non-public sources and methods), it attempts to issue most reports at the unclassified level and to the widest audience possible.

To better share information, the NIPC has spearheaded an aggressive outreach effort. NIPC officials have met with business, government, and community leaders across the United States and around the world to build the trust required for information sharing. Protection of business information and privacy interests are both stressed in NIPC internal deliberations and with business, government and community leaders. Most have been receptive to information sharing and value the information received from the NIPC. Others have expressed reservations due to a lack of understanding or perhaps confidence in the strength of the disclosure exceptions found in the Freedom of Information Act, concerns about whether the Justice Department would pursue prosecutions at the expense of private sector business interests, and simple reluctance to disclose proprietary information to any entity beyond their own control or beyond the direct control of the NIPC.

The annual Computer Security Institute/FBI Computer Crime and Security Survey, released in April, indicated that 90% of the respondents detected computer security breaches in the last 12 months. Only 34% reported the intrusions to law enforcement. On the positive side, that 34% is more than double the 16% who reported intrusions in 1996. The two primary reasons for not making a report were negative publicity and the recognition that competitors would use the information against them. Many respondents were not aware that they could report intrusions to law enforcement. We have moved aggressively to address these concerns and go out of our way to reassure businesses that their voluntarily provided information will remain secure, and that we are always sensitive to protecting the interests of victims who report crime.

WATCH AND WARNING

The NIPC Watch maintains a round-the-clock presence in the FBI's Strategic Information and Operations Center (SIOC). The Watch serves as the main portal into and out of the NIPC. Our recent advisory regarding the Klez.h worm was issued after the Watch received a voluntary report from a major telecommunications company. Following an analysis and consultations with our security partners, the NIPC issued Alert 02-2002: "W32/Klez.h @ mm Worm and Variants." Through the Watch, the Center produces and disseminates three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National Threat Warning System. Collectively, these warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact. If a particular warning is based on classified material that includes dissemination restrictions and contains information deemed valuable and essential for critical infrastructure protection, the NIPC will then seek to develop a sensitive "tear-line" version for distribution, including to critical sector coordinators, InfraGard members, and general law enforcement authorities. The three specific categories of NIPC warning products are as follows:

(1) "Assessments" address broad, general incident or issue awareness information and analysis that is both significant and current but does not necessarily suggest immediate action.

(2) "Advisories" address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

(3) "Alerts" address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

The main "audiences" that NIPC products can reach include: DoD, Federal civil agencies, the Intelligence Community, the Law Enforcement Community (including the state and local levels), FBI field offices and international Legal Attache offices, computer incident response centers, domestic and foreign cyber watch centers, private sector Information Sharing and Analysis Centers (ISACs), InfraGard members (see below for an explanation of the InfraGard program), and the general public.

Since its inception, the NIPC has issued over 100 warning products. A number of warning products have preceded incidents or prevented them entirely by alerting the user community to a new vulnerability or hacker exploit before acts are committed or exploits are used on a widespread basis. The Center has had particular success in alerting the user community to the presence of Denial of Service tools on the network and has in some cases provided a means to discover the presence of tools on a network. For example, in December 1999, as part of our Y2K efforts, the NIPC released a warning message along with a tool to allow users to find the presence of three specific denial of service tools on their systems. This was

something never before done by the government for the user community and occurred over a month before the Distributed Denial of Service Attacks of February, 2000. The NIPC's work with private companies has been so well received that the Systems Administrators and Network Security Organization (SANS-a trade group) awarded their yearly Security Technology Leadership Award to members of the NIPC's Special Technologies Applications Unit.

The NIPC is integrated into national level warning systems both through structures established by the National Security Council and by other agencies. Of particular note is the fact that the NIPC has been fully engaged in the planning and implementation of the interagency Cyber Warning Information Network (CWIN). Also of note: the NIPC, under the authority of the FBI, is the only locus where the widest range of law enforcement, counterintelligence, foreign intelligence, and private sector information may be lawfully collected, analyzed, and disseminated, all under well-developed statutory protections and the oversight of the Department of Justice. NIPC Advisory 01-003 and its companion NIPC Advisory 00-060, issued on March 8, 2001 and December 1, 2000, respectively, both on e-commerce vulnerabilities, are examples of warnings which effectively combine law enforcement, intelligence, and private sector information with the NIPC's warning mission. These advisories, coupled with a press conference on March 8, 2001, stopped over 1600 attempted exploitations by hackers. The advisories reflect the balance of information dissemination to the public with an ongoing law enforcement investigation, achieving both goals in the public's interest.

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT

With respect to sharing information within the government, PDD-63 mandates that government agencies will share information with the NIPC. The NIPC has established effective information sharing relationships across the U.S. Government. These arrangements are not always codified in formal interagency agreements or Memoranda of Understanding, but the important point is that they are working. The NIPC has also formed an Interagency Coordination Cell (IACC) at the Center which holds monthly meetings regarding ongoing investigations. To date, the IACC's growing membership has risen to approximately 35 government agencies that meet on a monthly basis to include representation from NASA , U.S. Postal Service, Air Force Office of Special Investigations (AFOSI), U.S. Secret Service, U.S. Customs, Departments of Energy, State and Education, and the Central Intelligence Agency, to name a few.

The IACC's accomplishments to date include the formation of several joint investigative task forces with member agencies participating, and over 30 separate instances of joint investigations of member agencies being initiated as a direct result of IACC meetings, information sharing and participation. In one case, an IACC member agency provided timely sensitive source information to the appropriate authorities which prevented the planned intrusion and compromise of another government agency's computer system and the preservation of critical log data used for the ensuing investigation.

The IACC's members are currently working on the establishment and development of a

database which would serve as a source of computer intrusion information compiled from member agency investigations to facilitate other investigations. It is also working on the establishment and administration of a dedicated virtual private secure network for member agencies to communicate vital infrastructure protection and computer intrusion information for immediate emergency response situations, in addition to dissemination of routine but sensitive information.

The Department of Defense has the second largest (after FBI) interagency contingent in the NIPC. The Deputy Director of the NIPC is a two-star Navy Rear Admiral; the Executive Director is detailed from the Air Force Office of Special Investigations; the Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service; the head of the NIPC Watch is a Naval Reserve officer; and the head of the Analysis and Information Sharing Unit is a National Security Agency detailee. There are also liaison representatives from the National Imagery and Mapping Agency and the Joint Programs Office. A contingent of DoD reservists serves in the Center to provide additional critical infrastructure expertise and emergency surge capabilities. NIPC works particularly closely with the DoD through liaison with the Joint Task Force-Computer Network Operations (JTF-CNO). NIPC members stay in close contact with their JTF-CNO counterparts, providing mutual assistance on intrusion cases into DoD systems, as well as on other matters. NIPC alerts, advisories, and assessments are routinely coordinated with the JTF-CNO prior to release to solicit JTF input. On several occasions, the NIPC and JTF-CNO have coordinated and issued joint cyber warnings on the same matter. There is also significant interaction with the military services, the Joint Staff, the Office of the Secretary, and other major DoD agencies.

Interagency managerial participation is by no means limited to DoD. For example, the Section Chief for Analysis and Warning is detailed from the Central Intelligence Agency, and the Assistant Section Chief for Computer Investigations and Operations is detailed from the U.S. Secret Service.

The NIPC also has an excellent cooperative relationship with the Federal Computer Incident Response Center (FedCIRC). The FedCIRC has detailed a person to our Watch Center in the past, and the NIPC's Director sits on FedCIRC's Senior Advisory Council. FedCIRC is operated by the General Services Administration as the central coordinating point on security vulnerabilities and lower level security incident data. In addition, the NIPC sends draft alerts, advisories, and assessments on a regular basis to FedCIRC for input and commentary prior to their release. NIPC and FedCIRC information exchange assists both centers with their analytic products. The NIPC and FedCIRC are currently discussing ways to improve the flow of information between the two organizations and encourage federal agency reporting of incident information. On several occasions, the two organizations have coordinated and issued joint cyber warnings.

More recently, in October of 2001, President Bush issued Executive Order 13231, which establishes the President's Critical Infrastructure Protection Board to "recommend policies and

coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems." EO 13231 expressed the current Administration's continued support of the NIPC's mission under PDD 63 and distinguishes the interagency entity from any particular Department by separately designating the Director of the NIPC to serve as a member of the newly created President's Board. The President also designated the Director of the NIPC to serve on the Board's Coordination Committee, together with only the Director of the Critical Infrastructure Assurance Office (Commerce); the Manager of the National Communications Systems (DoD); the Vice Chair, Chief Information Officers' (CIO) Council, NSA; and the Deputy Director of Central Intelligence for Community Management. Also of significance, President Bush specified within EO 13231 that the Board must work in coordination with the NIPC in connection with the following activities: (1) Outreach to the Private Sector and State and Local Governments; (2) Information Sharing; (3) Incident Coordination and Crisis Response; and (4) Law Enforcement Coordination with National Security Components.

Since 1998, the NIPC has been developing the FBI's Key Asset Initiative, to identify those entities that are vital to our national security, including our economic well-being. The information is maintained to support the broader effort to protect the critical infrastructures against both physical and cyber threats. This initiative benefits national security planning efforts by providing a better understanding of the location, importance, contact information and crisis management for critical infrastructure assets across the country. We have worked with the DoD and the Critical Infrastructure Assurance Office (CIAO) in this regard.

INTERAGENCY COORDINATION: FEDERAL, STATE AND LOCAL

Emergency Law Enforcement Services Sector

The NIPC has been designated by the Department of Justice/FBI to fulfill their responsibilities as the Sector Lead Agency with regard to Emergency Law Enforcement Services (ELES). The NIPC's efforts in this regard have served as a model for all other Sector Lead Agencies. More than 18,000 federal, state and local agencies comprise the ELES Sector. The NIPC serves as program manager for this function at the request of the FBI. Last year the NIPC completed the Emergency Law Enforcement Services Sector Plan; this was the first completed sector report under PDD-63 and was delivered to the White House in March 2001. Working with law enforcement agencies across the United States, the NIPC conducted a sector survey and used the results of this survey to draft a sector report. Responses from more than 1500 of these agencies to a sector-commissioned information systems vulnerability survey revealed that these organizations have become increasingly reliant on information and communications systems to perform their critical missions. The NIPC has also sponsored the formation of the Emergency Law Enforcement Services Sector forum, which meets quarterly to discuss issues relevant to sector security planning.

State Infrastructure Protection Center (SIPC) efforts

The NIPC, with its extensive experience in the areas of multi-agency and multi-disciplinary support to infrastructure protection efforts, is actively engaged in supporting similar models being created at the state and local level. The State of Texas has demonstrated itself as a leader in this area, and the NIPC, together with significant Department of Defense involvement, is actively facilitating their efforts. Over time, the NIPC expects to meet the challenge of serving as the US hub for infrastructure protection efforts not only in terms of full Federal government support, but also in terms of bringing together State and Local governments for a fully coordinated national response.

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT AND THE PRIVATE SECTOR

Infragard: The Most Extensive Network of Federal and Private Sector Partners in the World for Protecting the Infrastructure

The InfraGard program is a nationwide initiative that grew out of a pilot program started at the Cleveland FBI field office in 1996. Today, all 56 FBI field offices have active InfraGard chapters. Nationally, InfraGard has over 4000 members. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service the FBI provides to InfraGard members free of charge. It particularly benefits small businesses which have nowhere else to turn for assistance. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The InfraGard program received the 2001 World Safe Internet Safety Award from the Safe America Foundation for its efforts.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. InfraGard provides a mechanism for the public and private sectors to exchange information pertaining to cyber intrusion matters, computer network vulnerabilities and physical threats on infrastructures. All InfraGard participants are committed to the proposition that the exchange of information about threats on these critical infrastructures is an important element for successful infrastructure protection efforts. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

Private sector members and an FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership. The chapter members include representatives from the FBI, State and local law enforcement agencies, other government entities, private industry and academia. The National Infrastructure Protection Center and the Federal Bureau of Investigation play the part of facilitator by gathering information and distributing it to members, educating the public and members on infrastructure protection, and disseminating information through the InfraGard network.

InfraGard is responsible for providing four basic services to its members: secure and public WebSites, an alert and incident reporting network, local chapter activities, and a help desk. Under this program the FBI provides a secure electronic communications capability to all InfraGard members so that the NIPC can provide threat information to private industry owners and operators, and encourage private industry coordination with law enforcement, and each other, on cyber and related physical incidents. This will be accomplished by expanding the established separate WebSite and electronic mail system. The program anticipates at least 100 members in each chapter with further expansion as the program develops, with approximately 2,500 new members expected in calendar year 2002. A number of the larger field divisions anticipate starting several chapters in larger cities located in their respective geographic area of responsibility. The warnings that are provided to our InfraGard members improve the relationship between private industry and the local FBI offices due to the increased level of trust that is often established. It should be noted that the InfraGard program is not responsible for producing the alerts and warnings that are disseminated from the NIPC.

Information Sharing and Analysis Centers (ISACs)

The NIPC is continuing to reach out to the Information Sharing and Analysis Centers (ISACs). The NIPC has recently initiated the establishment of an ISAC Support and Development Unit, whose mission is to enhance private sector cooperation and trust, resulting in two-way sharing of information and increased security for the nation's critical infrastructures. The NIPC now has information sharing agreements with seven ISACs, including those representing energy, telecommunications, information technology, air transportation, water supply, food, and chemical sectors. Several more agreements are in the final stages. Just as important, the NIPC is receiving reports from member companies of the ISACs. The NIPC has proven to these companies that it can properly safeguard their information and can provide them with useful information. It is because of such reporting that the investigative caseload of the NIPC is burgeoning and more analytical products are being issued each year.

One example bears discussion. The North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC for an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the program have

stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information and the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. Additionally, some information available to the NIPC may be classified or law enforcement sensitive and, thus, unavailable to many in the industry. A group of NERC officials have been granted security clearances in order to access classified material on a need-to-know basis. Once the NIPC has determined that a warning should be issued, cleared electric power experts will be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide members of the industry with unclassified, nonproprietary, timely and actionable information to the maximum extent possible.

CERT/CC (a federally funded research and development corporation)

The NIPC and the Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Mellon University have formed a mutually beneficial contractual relationship. The NIPC receives information from the CERT (including advance Special Communications about impending CERT advisories, which CERT seeks NIPC input on, and weekly intrusion activity information) that it incorporates into strategic and tactical analyses and utilizes as part of its warning function. The NIPC's Watch and Analysis units are routinely in telephonic contact with CERT/CC and the anti-virus community for purposes of sharing vulnerability and threat information on a real-time basis. CERT/CC input is often sought when an NIPC warning is in production. The NIPC also provides information to the CERT that it obtains through investigations and other sources, using CERT as one method for distributing information to security professionals in industry and to the public. The Watch also provides the NIPC Daily Report to the CERT/CC via Internet e-mail. On more than one occasion, the NIPC provided CERT with the first information regarding a new threat, and the two organizations have often collaborated in disseminating information about incidents and threats.

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT AND INTERNATIONAL PARTNERS

The ability of the United States to assure homeland security clearly relies on the full participation and support of its international partners. It is with this in mind that the NIPC has promoted a wide array of international initiatives.

On the information infrastructure side of the equation, a typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Even intrusions into U.S. systems by a perpetrator operating within the U.S. often require international investigative activity because the attack is routed through Internet Service Providers and computer networks located outside the United States. When evidence is located within the United States, the NIPC coordinates law enforcement efforts which might include: subpoenaing records by FBI agents,

conduct of electronic surveillance, execution of search warrants, seizing and examining of evidence. We can not do those things ourselves to solve a U.S. criminal case overseas. Instead, we must depend on the local authorities to assist us. This means that effective international cooperation is essential to our ability to investigate cyber crime. The FBI's Legal Attaches (LEGATs) provide the means to accomplish our law enforcement coordination abroad, and are often the first officials contacted by foreign law enforcement should an incident occur overseas that requires U. S. assistance. NIPC personnel are in almost daily contact with LEGATs around the world to assist in coordinating requests for information.

International investigations pose special problems. First, while the situation has improved markedly in recent years, many countries lack substantive laws that specifically criminalize computer crimes. This means that those countries often lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist us when evidence might be located in those countries. Moreover, the quickly evolving technological aspects of these investigations can exceed the capabilities of local police forces in some countries. Finally, even when countries have the requisite laws and have developed the technical expertise necessary to conduct cyber investigations, successful investigation in this arena requires a more expeditious response than has traditionally been the case in international matters, because electronic evidence is fleeting and, if not secured quickly, can be lost forever.

The NIPC is working with its international partners on several fronts. The first area consists of outreach activities designed to raise awareness about the cyber threat, encourage countries to address the threat through substantive legislation, and provide advice on how to organize to deal with the threat most effectively. The Center often hosts foreign delegations to discuss topics ranging from current cases to the establishment of NIPC-like entities in other nations. Since the NIPC was founded, Australia, Japan, Israel, the United Kingdom, Canada, Germany, South Korea and Sweden have all formed interagency entities like the NIPC. The Center has established watch connectivity with similar centers in Australia, Canada, the United Kingdom, Sweden, and New Zealand; additionally, the Canada and the United Kingdom have each detailed a person full-time to the NIPC, and Australia detailed a person for 6 months in 2001. Currently, the Center is working jointly with the Department of State to develop and implement an international strategy for information sharing in the critical infrastructure protection arena. Finally, over the past year, the NIPC has briefed visitors from the United Kingdom, Australia, Canada, Germany, France, Georgia, Norway, New Zealand, Singapore, Bulgaria, Estonia, Latvia, Japan, Denmark, Sweden, South Korea, Israel, Italy, India, and other nations regarding critical infrastructure protection issues. These nations have all looked to the NIPC in order to create Critical Infrastructure Protection Centers of their own and to promote liaison on a bi-lateral basis between themselves and the United States, as well as with one another.

At the NIPC we continue to seek partnerships which promote two-way information sharing. As Director Mueller stated in a speech on April 19th, "Our top priority is still prevention." We can only prevent attacks on our critical infrastructures by building an intelligence base, analyzing that information, and providing timely, actionable threat-related products to our public and private sector partners. We welcome the efforts of your Committee in improving information sharing, and I look forward to addressing any questions you might have.

STATEMENT OF

JOHN G. MALCOLM

DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE COMMITTEE ON
GOVERNMENTAL AFFAIRS
U.S. SENATE

MAY 8, 2002

Mr. Chairman and Members of the Committee, thank you for this opportunity to testify about the Department of Justice's efforts to protect our nation's critical infrastructure and about information sharing related to that protection. The issues before this Committee today are of great importance, and I commend the Committee for holding this hearing.

In my testimony today, I would like to outline briefly the nature of critical infrastructure protection, the information sharing problem and the Department's current efforts to combat that problem. It is clear to the Department that information-sharing is a serious issue, and that its complexity presents a significant challenge to law enforcement.

The nature of the issue

The safety of our nation's critical infrastructure is of paramount concern to the Justice Department. As you know, the term "critical infrastructure" refers to both the physical and cyber-based resources that make up the backbone of our nation's telecommunications, energy, transportation, water, emergency services, banking and finance, and information systems.

The problem of ensuring delivery of critical infrastructure services is not new. Indeed, owners and operators of critical infrastructure facilities have been managing risks associated with service disruptions for as long as there have been such facilities. However, the operational challenge of ensuring the delivery of the broad array of services that now depend upon the Internet and other information systems is a challenge that has grown exponentially in the last several years. The burgeoning dependence of the U.S. infrastructure on the Internet has exposed vulnerabilities that have required the U.S. government to mount new initiatives, to create new federal entities to help manage critical infrastructure protection efforts, and to seek prevention, response, and reconstitution solutions.

The safety of our nation is our first and overriding objective. The Justice Department has been working across government to address infrastructure issues for several years. The attacks of September 11 heightened our awareness of these issues and have pushed us closer to resolution on some issues. Following those terrorist attacks, the Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act). That Act, which the President signed into law in October 2001, amended U.S. laws to further critical infrastructure protection efforts by increasing sentences for those committing cyber attacks, improving our ability to use procedural tools to track sources, and enabling law enforcement to share wiretap and grand jury information with others responsible for homeland defense when appropriate.

U.S. infrastructure protection efforts are the shared responsibility of many entities, both public and private. Much of this joint effort is based upon the principle that a robust exchange of

information about threats to and actual attacks on critical infrastructures is a critical element for successful infrastructure protection efforts. The following are just a few of the entities dedicated to this principle: the National Infrastructure Protection Center, the Department of Justice's Computer Crime and Intellectual Property Section, Information Sharing and Analysis Centers, the Critical Infrastructure Assurance Office, the Office of Homeland Security, and the Federal Computer Incident Response Center.

To better protect critical infrastructures, government and the private sector must work together to communicate risks and possible solutions. Acquiring information about potential vulnerabilities from the private sector is essential. Doing so better equips us to fix deficiencies before attackers can exploit them. For example, a telephone company might discover a vulnerability in a widely used component of our telephone network that makes the network susceptible to disruption by hackers. If we concentrate our time and energy on remediation of terrorist attacks after they occur, we have already lost. Information is the best friend of both prevention and response. We recognize that we can protect the nation only if the private sector feels free to share information with the government.

However, industry often is reluctant to share information with the Federal Government. One reason given by industry for not sharing information is that the government may later have to disclose that information under the Freedom of Information Act, or FOIA. Industry also is concerned that sharing information among companies will lead to antitrust liability, or that sharing among companies or with government will lead to other civil liabilities (e.g., through a

product liability suit or a shareholder suit). Without legal protections regarding information needed by the government in order to safeguard our infrastructure, even the most responsible, civic-minded companies and individuals may hesitate before sharing such crucial information, fearing that competitors may obtain that information and use it to their advantage.

With this in mind, both the Senate and the House of Representatives have actively considered and are currently considering bills that would specifically bar disclosure under the Freedom of Information Act of any information that is voluntarily submitted to government agencies to protect our critical infrastructure. Such a "corporate good Samaritan" law would provide the necessary legal assurance to those parties willing to voluntarily provide sensitive information to the government that they would not otherwise provide.

The Justice Department believes that the sharing of private sector security information on critical infrastructure between private sector entities and with the federal government to avert acts that harm, or threaten to harm, our national security is of the utmost importance. We are prepared to work closely with Congress to pass legislation that provides this important legal protection.

The Freedom of Information Act

Congress passed the Freedom of Information Act more than thirty-five years ago. FOIA established an effective statutory right of access to government information. The principles of government openness and accountability underlying FOIA are inherent in the democratic ideal.

However, achieving an informed citizenry is a goal that is sometimes counterpoised against other vital societal aims. Society's strong interest in an open government sometimes conflicts with other important interests of the public--such as the preservation of the confidentiality of sensitive commercial and governmental information. Though tensions among these competing interests are characteristic of a democratic society, their resolution lies in providing a workable formula that encompasses, balances, and appropriately protects all interests, while maintaining emphasis on the most responsible disclosure possible. It is this accommodation of countervailing public concerns, with disclosure as the predominant objective, that FOIA seeks to achieve.

The Freedom of Information Act generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that one of nine exemptions protects such records (or portions of them) from disclosure or they are protected by one of three special law enforcement record exclusions. Two exemptions are relevant here: 5 U.S.C. §§ 552(b)(3) and (4).

Exemption 4 of FOIA protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." The exemption affords protection to those business submitters who are required to furnish commercial or financial information to the government, either directly or indirectly, by safeguarding them from the competitive disadvantages that could result from disclosure. That exemption covers two categories of information in federal agency records: (1) trade secrets; and (2) information that is (a) commercial or financial, <u>and</u> (b) obtained from a person, <u>and</u> (c) privileged or confidential.

Exemption (3) of FOIA incorporates the disclosure prohibitions contained in various other federal statutes.

Case Law on Exemption 4

Over the years, a considerable body of law has developed, much of it in the form of decisions of the United States District Court for the District of Columbia and the Court of Appeals for the District of Columbia Circuit. In practice, the great majority of FOIA disputes revolve around whether the submitted information qualifies as "confidential" as that term has been judicially interpreted within the context of Exemption 4. It is important to recognize that the courts have regularly rejected any notion that either an information submitter's request for confidentiality, or an agency's promise that submitted information would not be released, by itself, suffices to insulate such information from disclosure under FOIA.

Under the District of Columbia Court of Appeals decision in Critical Mass Energy Project v. NRC, commercial information or information that is required to be furnished to the Government can be withheld primarily to the extent that the Government can demonstrate that its disclosure would result in "substantial competitive harm." However, where information is "voluntarily" submitted to the government, such information is protected to the extent that it is not "customarily" disclosed to the public by the submitter, a considerably easier standard to satisfy. It is our expectation that most information regarding critical infrastructure vulnerabilities will fall into the "voluntarily" submitted category and will, therefore, readily qualify for Exemption 4 protection under the DC Circuit's Critical Mass decision. At the same time, both we and business submitters are aware that this D.C. Circuit Court precedent might not

come to be accepted in all other judicial circuits, which gives rise to reasonable concerns.

Were the decision in Critical Mass a definitive legal principle decided by the United States Supreme Court, concerns regarding protection of this information would be greatly reduced. Since that is not the case, the Department recognizes that the broad protection afforded such information by the District of Columbia appellate court does not provide the complete assurances to the submitters of private sector infrastructure that they seek. Nor will protection be categoric in those instances in which information regarding vulnerabilities are included as part of a submission by state and local government entities.

Other Issues

Although FOIA is a major issue, it is not the only issue here. Some companies also claim that sharing information with the government, or each other, will lead to liability and possible antitrust suits by the government or by their competitors.

Legislative Action

The Department appreciates the continuing interest of the Congress. During the 106th Congress, bills were introduced in both the Senate and the House to address these issues. Both bills focused on protecting critical infrastructure information provided to the government from compelled disclosure under FOIA. Both bills also address the antitrust and liability issues.

Last session, Senators Bennett and Kyl again introduced a bill. Key provisions of their bill:

- shield from disclosure under FOIA, with a specific request by the company that submitted the information, critical infrastructure information voluntarily submitted to certain federal agencies;
- limit use of shared information in civil proceedings; and
- exempt critical infrastructure information-sharing activity from the antitrust laws.

Representatives Davis and Moran also introduced a new version of their bill. Although similar to the Bennett-Kyl bill, it more tightly restricts the government's use of such information. Later in the session, a consensus bill was developed, but not introduced.

Justice Department Concerns

Under the existing case law on Exemption 4 of FOIA, the Justice Department believes that critical infrastructure information submitted to the government should be protectible from disclosure. However, we realize that some in industry disagree or, at least, are lacking the certainty that allows them to comfortably submit information to the government with complete assurance that it will not be disclosed. Since the goal of our information sharing efforts is to increase information flow to the government, we need to address the concerns of these companies. Indeed, in a letter to the National Security Telecommunications and Advisory Committee last fall the President expressed his support for "a narrowly drafted exception to the Freedom of Information Act to protect information about corporations' and other organizations' vulnerabilities to information warfare and malicious hacking." An important point is that, without such a statutory provision, the government would never obtain the information, and,

thus, would not have it to disclose to begin under FOIA. Such a state of affairs, moreover, would not serve our vital national interests.

Scope of the Information Protected

By the same token, it is crucial that any bills be carefully crafted so as not to unnecessarily shield information. Defining critical infrastructure is difficult, and, on balance, the Department believes that a broad definition is better suited to this issue. Our objective is to reassure companies that appropriate information will be protected. Too narrow a definition may leave a company in doubt and result in the information being withheld from the government out of fear of FOIA disclosure, the very result we seek to prevent.

On the other hand, a bill that sweeps in too much information is just as bad. For example, suppose a bill were to protect all information (1) submitted by a person, (2) to a covered Federal agency, and (3) for informational purposes. If that were so, any information obtained by the EPA during a witness interview would likely be covered, since it would constitute information submitted by a person, to a covered Federal agency, for informational purposes. Such a bill would clearly cover too much information, and would not serve our national interests.

Three approaches are available to reduce this problem. First, drafters must make clear that any bill does not cover independently-obtained information. For example, let us suppose that a company submits valid critical infrastructure information to the Office of Homeland Security. Entirely independently, the EPA develops the same information in an investigation.

The government should be able to use the EPA's information without restriction. If this were not so, any information sharing bill would quickly turn into a shield, allowing companies to use the protections of the bill to dump information on the government and thus shield it for all time and for all purposes. In a sense, it is important to protect the "copy" of the information submitted to the government, but not the information itself.

Second, resolve the issue of who may receive the information in favor of designated agencies only. The choice here is between allowing any agency of the government to receive critical infrastructure information, or allowing only designated agencies or departments to receive it. We recommend that agency heads designate which components or bureaus, if any, may actually receive such information. This would provide for flexibility (agency heads could designate any appropriate office) and certainty (designated offices would know how to handle submitted information). This solution would also help prevent use of the Act as a sword–if an agency head did not want a component to receive protected information that might raise a question of immunity or improper use of voluntary submitted information, he or she could not designate that component.

Third, retain the provisions of the existing bills that require companies to voluntarily submit the information in order to obtain the protections of the bill. If the information is not so submitted–if it is instead produced in response to subpoena or a program requirement–the information is not covered. A voluntariness requirement is important because the goal of information sharing efforts is to encourage companies to share information that the government is not otherwise receiving.

We also suggest requiring that the submitter explicitly request the protection of the statute for two reasons. First, some information does not need protection, nor does industry want all information to be protected – yet all information would be automatically protected if no request is required. Second, a request will help the government identify the protected information, especially where such notification appears on the document itself.

Liability

As I mentioned earlier, FOIA is only the first of three issues raised by industry. The second issue relates to liability concerns. Some companies have expressed concern that, should they share information with the government, the government could then use that information in a civil or criminal suit against them. While perhaps legitimate concerns, let me be clear that the Justice Department would not support legislation that would prohibit the government from using voluntarily provided information in a criminal proceeding. Other mechanisms exist to give a company some consideration and possible benefit for voluntarily providing information about criminal violations. Some of these are outlined in the Justice Department's 1991 Policy on Voluntary Disclosures.

If Congress chooses to include civil liability protections, the protections must be very carefully crafted so as not to hamper, or even eviscerate, law enforcement objectives. The bills already introduced include civil liability provisions. Some drafts of the liability provision have included so-called "indirect" use protections. We strongly believe that, at most, only "direct" use should be prohibited, since indirect or derivative use is extremely difficult to disprove. A similar issue frequently lurks in immunity proceedings in criminal cases, where the Federal

government, in order to proceed with a criminal prosecution, may have to disprove derivative use of a defendant's statements in a so-called Kastigar hearing. In the civil context, for example, should the government receive information about a vulnerability under an information-sharing bill that included indirect civil protection and then seek to sue the submitter, we would be required to prove that the submitted information was not used in any way in the investigation, including developing leads. In essence, we have to prove that all of our evidence came from independent sources. Past experience clearly demonstrates that this is a very difficult burden to meet.

State Laws

As you know, infrastructure protection efforts are a cooperative effort among the Federal Government, industry, and State and local governments. Any information sharing bill needs to consider how and when information may be shared with State and local governments. All States have their own FOIA or sunshine laws, which vary widely. It would make little sense to protect the information federally but leave it subject to disclosure under State FOIA laws once shared with States.

Antitrust Issues

The third of the issues raised by industry are antitrust concerns. Historically, the Justice Department has viewed requests for antitrust exemptions from the private sector as unnecessary, since they are unlikely to violate the antitrust laws. However, an exemption with respect to critical infrastructure protection is being discussed within the Administration.

Conclusion

Mr. Chairman, I want to thank you again for this opportunity to testify about our efforts to protect critical infrastructure. Citizens are deeply concerned about their safety and security of our country. By addressing information sharing, Congress will enhance the ability of law enforcement to fight cybercrime, terrorism, and protect our infrastructure. The Department of Justice stands ready to work with the Members of this Committee to achieve these important goals.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.

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 protection – information sharing.

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 to protect the public, safeguard the integrity of economy, and ensure 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, infrastructure security is about 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 protection. Establishing this trusted environment is no small challenge.

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 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. However, where potential legal and regulatory obstacles may unduly impede information sharing or otherwise interfere with the business community's efforts to maximize security efforts, it is incumbent on government to take appropriate steps to address them and correct them, as appropriate.

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 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, when 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 such operations will be conducted in compliance with applicable law and regulation.

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 hold 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 FBI 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 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 serve to 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.

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. Since last fall, legislation has been introduced to address these concerns. These bills highlight many of the complex and important issues facing the nation.

HOW CAN LEGISLATION CONTRIBUTE TO ENCOURAGING EFFECTIVE INFORMATION SHARING?

Legislation can help by clarifying and making more predictable the consequences of security information sharing with industry and with the government. 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. A FOIA exemption is necessary but not sufficient to increase information sharing. The critical factor is trust, and a FOIA exemption can help create a foundation of 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 in a manner that assures that it not then be released publicly under state sunshine laws. 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.

Testimony of
Michehl R. Gent, President and Chief Executive Officer
North American Electric Reliability Council

Hearing Before the United States Senate
Committee on Governmental Affairs

May 8, 2002

SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC INFORMATION SHARING

Summary

- The electric industry operates in a constant state of preparedness. Planning, training, and operating synchronous (non-switchable) grids prepares the electric industry for natural disasters such as earthquakes, floods, tornados, energy emergencies, and attacks of sabotage and terrorism.

- The North American Electric Reliability Council (NERC) serves as the electric industry's contact and coordinator in the United States and Canada for bulk electric system security matters and is the Electricity Sector's Information Sharing and Analysis Center (ES-ISAC).

- NERC has elevated critical infrastructure protection to be the focus of a high-level advisory group comprised of all ownership segments in the electric industry. The Critical Infrastructure Protection Advisory Group (CIPAG) reports directly to NERC's Board of Trustees.

- Infrastructure protection is a high priority for those who operate electric systems. CIPAG is the electric industry's primary organization for coordinating with government agencies and for oversight of NERC activities relating to critical infrastructure protection.

Recommendations

- Provide a way for sponsoring agencies, such as the FBI and DOE, to increase the number of industry personnel with security clearances. Private industry input is needed for credible vulnerability assessments.

- Provide inexpensive, effective, secure communications tools for industry participants in infrastructure ISACs.

- Provide limited, specific exemptions from the Freedom of Information Act restrictions for certain sensitive information shared by the private sector with the federal government. Provide narrow antitrust exemption for certain related information-sharing activities within the industry. S. 1456 achieves this result.

- Adopt the reliability legislation recently passed by the Senate as part of the comprehensive energy bill.

Background

My name is Michehl R. Gent, and I am President and Chief Executive Officer of the North American Electric Reliability Council. NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. NERC comprises ten Regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC works with all segments of the electric industry — investor-owned utilities; federal power utilities; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; and power marketers — as well as end-use customers, to "keep the lights on" by developing and encouraging compliance with rules for the reliable operation of the electric system. NERC also works closely with the federal government agencies to ensure that the nation's critical infrastructure protection programs are implemented throughout the electric industry.

I am responsible for directing NERC's activities both within the electric industry and between the electric industry and the federal government as these activities relate to physical and cyber terrorism of the electric systems of North America. NERC has served on a number of occasions as the electric utility industry's primary point of contact for issues relating to national security. This began in the early 1980s when NERC became involved with the electromagnetic pulse phenomenon. Since then, NERC has worked with the federal government to address the vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Year 2000 rollover impacts, and most recently the threat of cyber terrorism. At the heart of NERC's efforts has been a commitment to work with various federal agencies including the National Security Council (NSC), the Department of Energy (DOE), the Nuclear Regulatory Commission (NRC), and the Federal Bureau of Investigations (FBI) to reduce the vulnerability of interconnected electric systems to such threats. We hope to continue this high record of achievement by working effectively with the Office of Homeland Security.

NERC's long history of coordination with the federal government on grid security enabled the electric industry to respond rapidly and effectively to protect the nation's electricity production and delivery infrastructure in response to the terrible events that occurred last September. NERC maintains a close working relationship with the FBI's National Infrastructure Protection Center (NIPC) and the Department of Energy's Emergency Operations Center (DOE-EOC), and participates and hosts several related critical infrastructure protection programs, including the NERC Critical Infrastructure Protection Advisory Group (CIPAG); the Indications, Analysis, and Warnings Program (IAWP); the Electricity Sector Information Sharing and Analysis Center (ES-ISAC); and the Partnership for Critical Infrastructure Security (PCIS). In that same vein, NERC stands ready and able to work closely with the new Office of Homeland Security, under the leadership of Governor Tom Ridge.

In this testimony I will discuss NERC's activities on behalf of the electric industry and demonstrate that, through planning, hard work, coordination and cooperation, and effective communications, the electric industry is prepared for catastrophic events, even events as unthinkable as those that occurred on September 11, 2001. I will also discuss how information flows within the industry, and to and from industry and government. I will also discuss how the electric industry is working with the government to protect the electricity supply system against future physical and cyber attacks.

Electric Industry Response to the Terrorist Attacks of September 11, 2001

On the morning of September 11, NERC was notified that there had been apparent terrorist attacks on the World Trade Center (WTC). At about 10 a.m., NERC asked its 21 Reliability Coordinators and underlying control areas to go to "full-alert" status. Over the next several hours, NERC established contacts with the FBI, the NRC, and DOE's EOC. NERC then tested our security-related communications channels, which were operating normally. NERC communicates with its Reliability Coordinators via an Internet communications system and a private frame-relay system. We also have a secure telephone-based communications system with certain federal agencies. Throughout the day we maintained constant contact with the NERC Reliability Coordinators and continued to monitor system status across the continent. The immediate impact of the WTC attacks was the loss of electric service to lower Manhattan; approximately 400 MW of load on Consolidated Edison's system was lost. As catastrophic as this event was, it was locally contained from an electrical standpoint. The local systems worked as they were designed in accordance with local and regional reliability criteria, and at no time was the larger electric grid in any danger.

On the morning of September 12, I participated in an FBI briefing. Following that briefing and based on information received from the FBI, NERC moved its Reliability Coordinators to alert-level 2, which constitutes a heightened state of readiness but less than full alert. Since September 11, NERC has codified its alert levels in two documents: Threat Alert Levels and Physical Response Guidelines and Threat Alert Levels and Cyber Response Guidelines. Both documents were developed through a collaborative process in which all industry stakeholders participated. Today, the electric industry is at "Threatcon-low," which acknowledges the existence of a general threat of terrorist or increased criminal activity with no specific threat directed against the electric industry. The industry will remain at this level for both physical and cyber threats until NERC receives intelligence that this state of readiness is no longer appropriate.

On September 13, NERC initiated daily Reliability Coordinator calls. The FBI and EOC also participated in those calls. Those calls were in addition to the daily calls conducted by regional operators to discuss operations issues. Today, those daily calls between the ES-ISAC, NIPC and DOE-EOC continue.

On September 17, distributed denial of service (DDoS) cyber attacks started, and they continued for about a week. Several servers connected to the Internet were targeted and eventually shut down for a few hours. To my knowledge, no facilities connected with the operation of the bulk electric system, or connected with customer billing information, were

affected. On Tuesday, September 18, the now infamous NIMDA virus was unleashed. While widespread disruptions again were experienced, no electric control systems were affected.

Preparedness for Terrorism is Not New

The industry was well prepared to deal with events such as those of September 11, 2001. In 1988, NERC worked with the National Security Council, as directed by the Vice President's Task Force on Terrorism, to create a Generic Security Program, a Facility Program, and an Operations Program to combat multi-site, state-sponsored terrorism. Those activities resulted in 12 recommendations. The most important were that each operating entity must (1) have a plan that is exercised regularly in conjunction with all the other operating entities in the region, and (2) establish a contact with the local FBI office. These plans were in place and were implemented on the morning of September 11. Many of the other recommendations are also in place, such as a spare transformer database, a proper names database maintained for the FBI, changes to the operating standards to recognize sabotage and terrorism events, and an enhancement of our notification networks.

Another development in the mid-1990s that proved to be critical during the 9/11 crisis was the creation of 21 NERC Reliability Coordinators across North America. Reliability used in this context means the operation of the high-voltage transmission systems to ensure that reliability and grid integrity is maintained throughout all conceivable single contingencies. These Reliability Coordinators are responsible for seeing and understanding the big picture in terms of bulk electric system operations. They assess the moment-to-moment reliability of the grid and take actions to maintain transmission system reliability. Reliability Coordinators are authorized to call on transmission loading relief procedures or take other steps to ensure that commercial energy transactions do not overload the grid beyond NERC-established reliability criteria. These 21 Reliability Coordinators are also responsible for coordination during emergencies, and operate 24 hours-a-day, 7 days-a-week. I commend the NERC Reliability Coordinators for their extraordinary dedication and responsiveness, which was again demonstrated during the national emergency of 9/11.

The report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to a May 1998 Presidential Decision Directive (PDD-63). PDD-63 called for government agencies to become involved in the process of developing a National Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical systems through public-private partnerships. The PCCIP specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. In September 1998, then Secretary of Energy Bill Richardson sought NERC's assistance in developing a program for protecting the nation's critical electricity sector infrastructure and NERC agreed to participate as the electricity sector coordinator.

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison worked through its Infrastructure Assurance Outreach Program to help the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. The product of this effort forms the basis of NERC policy on information assurance. In addition, DOE provided clearances for a number

of industry personnel to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America. These clearances complement those obtained from the FBI.

On at least two occasions, Congress has asked the General Accounting Office (GAO) to study the practices of organizations that successfully share sensitive information. GAO report B-247385, April 1992, "Electricity Supply, Efforts Under Way to Improve Federal Electrical Disruption Preparedness," and GAO report GAO-02-24, October 15, 2001, "Information Sharing: Practices That Can Benefit Critical Infrastructure Protection," outline and report on many of the ways in which NERC coordinates industry response activities.

Future Actions

To continue the success of the systems and programs we have in place to ensure the secure operation of the bulk electric system, NERC is examining all of our policies, standards, practices, and procedures that specifically apply to operator readiness and response to terrorism, both physical and cyber. As a result of the 9/11 attack, we have:

- asked our Compliance Enforcement Program people to quickly assess the industry's state of compliance with the standards that directly apply to terrorism.
- established a work team to identify "security risk" documents and web sites, with an eye to ensuring that critical system information does not get into the wrong hands. That team is now part of CIPAG.
- protected NERC web sites that show critical information such as real-time power flows over critical paths against those who merely may be curious, as opposed to those that rely on this information for legitimate reliability or commercial purposes.
- attained assurances from operating entities that their security plans are appropriately updated and are being routinely exercised.
- worked to ensure closer coordination between those entities responsible for physical systems and those responsible for cyber security. In the past, these activities were often addressed separately. Many electric industry organizations have reorganized to combine physical and cyber security under the same management.
- worked to reaffirm and improve our contacts with the FBI, DOE, and other government agencies.

In the longer term, we need to guarantee that NERC has the full complement of tools necessary to ensure the continued reliability of the electric grid. We need Congress to pass the reliability legislation included as part of the comprehensive energy bill recently passed by the Senate. That legislation would provide for an industry self-regulatory electric reliability organization (ERO) to set and enforce mandatory reliability rules. That matter is presently before the House-Senate Conference Committee in H.R. 4. Presently, the NERC reliability rules and the security procedures that we have in place throughout the industry are essentially

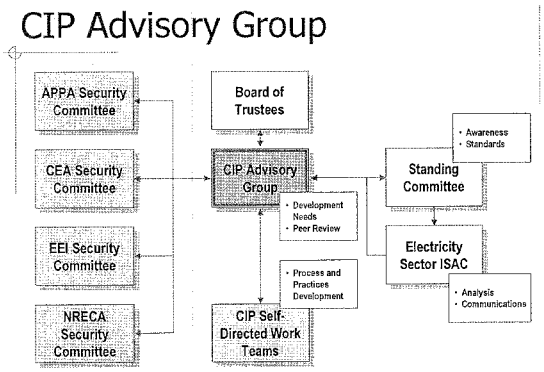
voluntary rules with no provision for enforcement. Only with mandatory enforceable standards can NERC ensure the secure and reliable operation of the bulk electric systems. NERC and most organizations representing electricity consumers, states, and utilities believe that an ERO is best situated to develop and enforce bulk power system reliability standards throughout North America. The President's National Energy Plan also endorsed the creation of an ERO, subject to Federal Energy Regulatory Commission (FERC) oversight in the U.S.

In the months ahead, our industry-based CIPAG will continue to work with government to better ensure the security of our nation's critical infrastructures. This means working closely with the new Office of Homeland Security. I personally believe that a Y2k-type of approach will be the most effective way to get the commitment of the 3,600 entities that together operate the electric grids in the United States and Canada to deal effectively with all aspects of physical and cyber terrorism. The efforts put forth by our industry in response to the Y2k threat demonstrated unmatched and unprecedented cooperation within the industry and with government. Those activities provide a strong model upon which any new infrastructure protection actions should be based.

Critical Infrastructure Protection Advisory Group

NERC created CIPAG to evaluate sharing cyber and physical incident data affecting the bulk electric systems in North America. This Advisory Group, which reports to NERC's Board of Trustees, has Regional Reliability Council and industry sector representation as well as participation by the Critical Infrastructure Assurance Office in the Department of Commerce (CIAO), DOE, NIPC, and FERC.

It is essential that all Electricity Sector segments be represented in the Critical Infrastructure Protection (CIP) development process. The participants include the dedicated experts in the Electricity Sector who represent physical, cyber, and operations security. NERC is recognized as the most representative organization of the Electricity Sector for this coordination function, as demonstrated by NERC's performance as project coordinator for the Electricity Sector for the Y2k transition. The security committees and communities associated with industry organizations (American Public Power Association, Canadian Electricity Association, Edison Electric Institute, and National Rural Electric Cooperative Association) provide the expertise for physical security in the Electricity Sector to compliment NERC's existing operational and cyber security expertise. The Advisory Group relies on small self-directed working teams, a proven and effective method for developing detailed processes and practices by subject matter experts, concluding with peer review in the forum environment.



Activities

CIPAG activities are conducted so as to reduce the vulnerability of the North American bulk electric system to the effects of physical and cyber terrorism. The Advisory Group's activities include developing recommendations and practices related to monitoring, detection, protection, restoration, training, and exercises.

Specific activities include:

- Identifying and coordinating with groups responsible for both physical and cyber security in all Electricity Sector segments. The organizations include APPA, CEA, EEI, ELCON, EPRI, EPSA, and NRECA.
- Provide oversight and assistance to NERC in its DOE-designated responsibility as the Electric Power Sector Coordinator, and provide liaison with government agencies.
- Recommending to the NERC standing committees on any needed modifications to NERC reliability standards dealing with emergency operations, disturbance reporting, and other CIP-related issues.
- Developing procedures for data exchange with government agencies.
- Providing oversight to the ES-ISAC.
- Maintaining the Indications, Analysis, and Warnings Program with NIPC.

- Maintaining the Electricity Sector's Security Alert Levels.
- Providing oversight and support to the Electricity Sector's representative on the PCIS.

Security Guidelines for the Electricity Sector

NERC's Approach to Action defines the need to address security. Last October, CIPAG began to compile "best practices" that electricity sector entities could consider when developing and implementing their security plans. The effort resulted in a document titled *Security Guidelines for the Electricity Sector,* which is pending approval of NERC's Board of Trustees.

The guidelines describe general approaches, considerations, practices, and planning philosophies in the following subject areas:

1. Vulnerability and Risk Assessment
2. Threat Response Capability
3. Emergency Management
4. Continuity of Business Processes
5. Communications
6. Physical Security
7. Information Technology/Cyber Security
8. Employment Screening

Recognizing that specific programs or implementation of security considerations must reflect an individual organization's assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk, the guidelines offer specific activities that may be undertaken in each of the subject areas.

National Infrastructure Protection Center Activities

NERC has a close working relationship with NIPC. The electric industry has worked closely with NIPC for about two years to develop a voluntary, industry-wide physical and cyber security indications, analysis, and warning reporting procedure. This program provides NIPC with information that, when combined with other intelligence available to it, allows NIPC to provide the electric industry with timely, accurate, and actionable alerts and warnings of imminent or emerging physical or cyber attacks. A high degree of cooperation with NIPC is possible because of the industry's long history of working with local, state, and federal government agencies. In the late 1980s, the NERC Board of Trustees directed the NERC staff to establish and maintain a working relationship with the FBI at the national level. The Board also resolved that each electric utility should develop a close working relationship with its local FBI office, if it did not already have such a relationship. The existence of these relationships was a critical element in ensuring the industry's coordinated and effective response to the terrorist attacks of September 11.

Indications, Analysis, and Warnings Program

One of CIPAG's first tasks was to develop the incident data types and event thresholds to be used in an information-sharing program with NIPC. Information sharing (electronic and telephone) mechanisms have been developed for use by electric transmission providers, generation providers, and other industry entities for reporting on a voluntary basis to both NIPC and NERC. Assessments, advisories, and alerts prepared by NIPC (with NERC's support), based on the data provided by the electric and other industry sectors and government sources, will be stated in an actionable manner and will be transmitted to electric industry entities. This process was tested successfully within one Regional Reliability Council during the fall and winter of 1999/2000. Because some of the analyses involve classified information, U.S. government security clearances have been obtained by key industry personnel and NERC staff members. Other electric industry personnel are in the process of obtaining security clearances. It would be useful for Congress to provide a way for sponsoring agencies, such as the FBI and DOE, to increase the number of industry personnel with security clearances.

The Indications, Analysis, and Warnings Program (IAWP), which evolved from this work, was implemented in July 2000; initial emphasis is on reporting by NERC Reliability Coordinators and utility control areas. Individual electric utilities, marketers, and other electricity supply and delivery entities are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings and related materials. Workshops have been conducted to provide program details to the industry, and a more comprehensive communications program is being developed by CIPAG to encourage broader industry participation in the program. The IAWP is a key voluntary first step toward preparing the electricity sector to meet PDD-63 objectives.

Electricity Sector Information Sharing and Analysis Center

The President's Commission on Critical Infrastructure Protection recommended that each of the critical infrastructure sectors establish an Information Sharing and Analysis Center (ISAC) to help protect the infrastructures from disruption arising from coordinated intrusion or attack. The ISACs gather incident data from within their respective sectors, perform analysis to determine potential malicious intent, share findings with other ISACs (private and government) in a manner that ensures, as required, target identity protection, and disseminate actionable warnings so appropriate action can be taken within each sector. ISACs serve as points of contact between sectors to facilitate communications, especially during a time of stress. ISACs study cross-sector interdependencies to better understand and be prepared for the possible impacts of an "outage" in one sector or another.

NERC is the Electricity Sector ISAC that performs essentially the same functions that have been required of NERC for physical sabotage and terrorism. The ES-ISAC's duties are:

1. Receive voluntarily supplied incident data from electric industry entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.

3. Assist the NIPC personnel during its analyses on a cross-private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts and other related materials to all those within the electric industry who wish to participate.

The ES-ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will request support for a 24-hour, seven-days-a-week staffed facility. NERC has established relationships with the other ISACs through the PCIS (see below) and will establish relationships with other ISACs as they form.

Information sharing of sensitive information among operating entities and with the ES-ISAC is seriously limited by the unavailability of communications equipment that would allow secure voice conversations. Secure communications is limited to encrypted e-mail.

Critical Infrastructure Protection Planning

The CIPAG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the electric industry. Separate business cases as well as a general overview have been prepared for chief executive officers, chief operating officers, and chief information officers. The purpose of the business case is to persuade industry participants to report incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPAG has developed a basic and fairly comprehensive plan to address CIP. The prototype plan, still undergoing industry review, addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, restoration, and interdependencies between and among sectors.

The essence of this "Approach to Action" is being considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government.

Several documents related to critical infrastructure protection can be found at http://www.nerc.com/~filez/cip.html.

Partnership for Critical Infrastructure Security

The PCIS was established to promote public/private cooperation and communication. It is supported by CIAO and the U.S. Chamber of Commerce. In 2001, PCIS was established as a not-for-profit organization and elected a Board of Directors and company officers. NERC participates in PCIS and I serve as its Secretary. Its stated mission is to coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to the economy and the nation's critical infrastructure.

PCIS is focusing its efforts on these functional areas:

- Interdependency Vulnerability and Risk Management
- Information Sharing
- Public Policy Issues
- Research and Development
- National Strategy

Through these activities we will gain a clearer understanding of sector interdependencies, better communication between sectors via ISACs and with public stakeholders, increased sharing of common research and development efforts, and ultimately coordinated efforts to protect our nation.

Improvements to Information Sharing

As positive and useful as these activities have been, however, there is yet more information that could be provided to the government in order to assist it in helping the private sector understand such complicated potential vulnerabilities as the interdependencies between and among different infrastructures, such as telecommunications, electricity, transportation, and natural gas.

Problems Associated With Information Sharing

Any information-sharing activity, however, voluntary or not, raises serious security concerns. In particular, any time that the government has access to what is, in essence, "targeting" information, there is the risk that some hostile agent could also gain access to it and use it to do great harm. The problem becomes even more acute when information is not only required to be made available, but is then published on the internet in real time, providing easy access to anyone looking to identify weak links in the utility grid. Of course, legitimate market participants and regulators need to obtain information in a timely manner, but access to truly sensitive information must be strictly controlled.

A corollary problem exists regarding whether and how to create a structure and process for the industry to work together in order to share information and analysis, and to plan for resisting, responding to, and recovering from hostile activity. I am not an expert on the Freedom of Information Act (FOIA) or antitrust law (or even a lawyer), but I have many years of practical experience in this industry. Based on that experience, I understand that company executives and managers believe they cannot prudently discuss certain matters with their competitors, suppliers, or customers. They believe that such discussions, and especially any resulting plans or actions, could be the source of antitrust litigation. In addition, even if the company might ultimately prevail, the great expense, potential risk of adverse publicity or even temporary loss, and possible public release of sensitive information during the course of such litigation lead them to not even begin the conversation in the first place. That diminishes our ability to improve our security in advance of a problem.

These concerns go beyond the potential antitrust problems caused by merely sharing information about threats. In particular, entire industries are now having to address whether and how to share spare parts or other resources to repair major, widespread damage and prevent worse calamities due to cascading failures. The issue of sharing also involves potential allocations of scarce commodities — both supplies for repair, and products for customers. Further, entire industries may determine security-related requirements to ask of their suppliers and business partners. At the least, entire industries may discuss the security-related shortcomings of existing products, suppliers and partners. Each of these actions is ripe for allegations of illegal market manipulation (boycotts, market allocations, etc.).

These issues are not simply theoretical. DOE and OHS have asked the electric utility industry to provide the government with a list of nationally critical electric facilities. We can imagine several reasons why various agencies and levels of government each might have their own needs to be aware of the industry's most critical facilities. Certainly, the industry has been expanding its critical facilities database for its own management purposes over the last several months. However, we cannot simply ignore the security concerns we have been voicing since the mid-1980s and hand over even a small part of any such database without adequate assurance that such information will receive appropriate protection. Neither is it clear that a bare list created for the federal government's purposes would contain the same information as an industry-created list, or would have any benefit at all to the industry.

What Government Can Do to Encourage Information-Sharing

We are asking federal regulators, agencies, and states to reconsider what information they request of utilities, especially market information identifying system constraints and the availability of critical facilities. Our industry has especially asked that they reconsider how they share that information once they obtain it. In fact, the Federal Energy Regulatory Commission (FERC) is beginning to address those issues. FERC recently asked for advice and suggestions on how to prevent sensitive information from being disclosed despite the requirements of FOIA. However, there is no clear process or timeline for any final decision by FERC.

Congress is in the best position to mitigate the security risks inherent in information-sharing activities, whether voluntary or required. As to voluntary information-sharing, Senators Robert Bennett (R-UT) and Jon Kyl (R-AZ) have introduced legislation, S. 1456, that would promote voluntary information sharing about sensitive security issues among infrastructure companies, and between those companies and the government by providing limited, specific clarifications of the Freedom of Information Act (FOIA) and of federal antitrust laws for certain critical infrastructure protection information sharing efforts by the private sector. I have been informed that this proposal builds on existing relevant legal precedents such as the 1998 Y2K Information and Readiness Disclosure Act, the 1984 National Cooperative Research Act, certain (territorially limited) court rulings, as well as a very few, case-specific Department of Justice advisory letters.

Similar, bipartisan legislation, H.R. 2435, has already been introduced in the House by Representatives Tom Davis (R-VA) and James Moran (D-VA). Our industry is part of a coalition of critical infrastructure industries that strongly supports the efforts to combine these

two proposals, and we urge Congress to promptly enact the product of those efforts. The proposed legislation would be a clear statement from the government that such information-sharing organizations and activities are not only permissible, but are actively encouraged. Congress can also help mitigate security risks by providing similar direction to federal agencies and the states regarding Federal and state requirements for reporting and public dissemination of critical, sensitive data, especially information identifying system constraints and the availability of critical facilities.

Conclusion

In conclusion I would like to make three points:

- The physical properties of the interconnected electric grids require close coordination and adherence by operating entities and users of these grids to the common reliability rules. Our 34-year history of cooperation and coordination has served the industry, the United States, and Canada well. As a result, I believe the electric industry is the best prepared of all the infrastructure industries.

- Coordination and cooperation among all electric industry participants and coordination with government agencies through the Regional Reliability Council concept has been the key to this success.

- The Critical Infrastructure Protection Advisory Group plays the central role in coordinating electric industry actions to promote critical infrastructure protection.

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.

---

[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.

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 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. 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.

Testimony of Harris N. Miller
President, Information Technology Association of America
May 8, 2002
Before the
United States Senate

APPENDIX 1:
Focus on the Freedom of Information Act
Reasons Current Law Fails to Adequately Protect Critical Infrastructure Threat Information

The Freedom of Information Act (FOIA, 5 USC 552) expresses the policy of the United States in favor of disclosure of information in the government's possession, to the greatest possible extent. No one argues with this basic premise of government in America. Transparency and open government are important parts of the foundation of our democracy.

At the same time, no one disputes that when the government engages in strategic planning and discussions about the national security and national defense in the emerging and dangerous world spawned by the resurgence of Terrorism and the necessity of making War on it, the sensitive information generated should be exempt from disclosure on grounds of overriding national defense and foreign policy considerations.

In addition, no one disputes that the "Critical Infrastructure" of the United States – from pipelines and electric utilities to information networks and telecommunications, transportation systems for goods and people and more -- is at risk of attack both prior to, and now, during the War on Terrorism.

The bulk of this Critical Infrastructure, however, is under the ownership and control of America's private sector, not the national security umbrella of government. It is time to recognize the important role in national security and foreign policy that America's Critical Infrastructure plays, and treat information related to "any threat to the security of critical infrastructure" just as any other information exempt from disclosure as a matter of national security.

That is not the case today. Information generated by the government and properly classified under "criteria established by an Executive order to be kept secret in the interest of national security or foreign policy" is exempt from disclosure. Period. 5 USC 552 (b)(1)(A)(B). Information generated by the private sector owners and operator's of the nation's Critical Infrastructure and voluntarily shared with a government agency may be treated as "confidential business information" [1], but only if the agency makes a number of determinations in its discretion, and it does not exercise its discretion to

[1] The statutory phrase is "trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 USC 552 (b)(4).

change its mind in the future. Such information may also fit within the FOIA exclusion for "law enforcement information" when disclosure "could reasonably be expected to endanger the life or physical safety of any individual" (5 USC 552(b)(7)(F)), but the same reservations about agency discretion apply here as well. Treatment of Critical Infrastructure threat information should be "upgraded" by providing that it is specifically exempted from disclosure by statute (5 USC 552(b)(3)) removing the extra burden of discretionary treatment.

The change will not open the floodgates to a host of other exemptions from disclosure. This change would respond to a limited need for specific relief in the case of information that rises to the level of a national security concern, but resides outside the national security umbrella. It does not seem likely that other requests for new exemption could meet this test.

It should be the case that upgrading this specific type of information is in the interest not just of the business community, but also of the government itself and the citizenry in general. It is in everyone's interest to take the steps reasonably necessary to protect Critical Infrastructure from attack, and learn from incidents and recoveries that have taken place in the past.

What is clear is that current FOIA treatment of Critical Infrastructure Threat Information makes the private sector reluctant to engage in the full and frank disclosure of information to government that should be taking place right now. Why is the current FOIA treatment of Critical Infrastructure Threat information less than adequate? There are a number of reasons. Here are several:

1. Under current rules the submitter of information does not know whether it will be treated as confidential by the agency, and the agency will not make a commitment at the time of submission. This lack of certainty alone prevents many disclosures.

2. Current policy requires that agencies not exercise their discretionary authority unless and until a disclosure request under FOIA is received. When a request is received, agencies have discretion to inform the submitter of the need to defend the confidentiality of their information. The agencies can decide they have enough information to make the decision without informing the submitter.

3. Recent precedents (the Critical Mass case and its progeny) suggest that "voluntarily" submitted "trade secret, commercial or financial information" may be protected from disclosure if not "customarily" disclosed by the submitter. Nevertheless, every word in quotes represents a different discretionary determination that must be made by the agency at the time of a FOIA request. Submitters have their arguments to make, but no assurance that those arguments will be accepted.

4. Recent precedents are not necessarily accepted throughout the United States in every judicial circuit. Submission of critical infrastructure threat information should not be expected to be limited to agencies in Washington, D.C.

5. Information disclosed to competitors in an ISAC under the terms of binding non-disclosure agreements (NDA) conditioning ISAC membership may qualify for confidential treatment under the Critical Mass case, but absent strict compliance with such formal requirements – as could happen in the case of an incident recovery crisis or other emergency – disclosure by the submitter could lead to a finding that Critical Mass protections do not apply.

6. Agencies always have discretion to decide that, despite a submitter's claim of confidentiality and the reasons for it, the submitter's claim in light of the passage of time or other considerations cannot be valid and the policy interests expressed by FOIA are stronger and enough to justify disclosure. That is a risk the business community has come to accept in its ongoing dialogue with government. It is not a risk that should have to be assumed for the treatment of critical infrastructure threat information.

7. Some confidential business information turns stale with the passage of time, justifying the exercise of agency discretion. Critical infrastructure threat information does not. That alone should be reason enough to upgrade its treatment under FOIA.

In sum, it is essential to eliminate discretionary treatment for this limited class of information. The owners and operators of the nation's critical infrastructures should be able to have confidence that the information they share with government will not be made public at a later date. Today they do not have that confidence.

Testimony of Harris N. Miller, President
Information Technology Association of America
May 8, 2002
Before the Committee on Government Affairs
United States Senate

APPENDIX 2:
Focus on Business Review Letters at the Department of Justice
Reasons Current Practice Fails to Adequately Address Sharing Critical Infrastructure Threat Information within the Private Sector

There is broad agreement that the strong policy against anticompetitive practices in restraint of trade, expressed in the nation's antitrust laws, is a basic premise of American law and economic life. Vigorously enforced antitrust laws are fundamental to the success of the American economy in the emerging integrating world.

At the same time there is a general understanding that the broad mandates of the antitrust statutes, coupled with over 100 years of judicial precedent, congressional amendment and federal regulation, can lead to ambiguous interpretations of the coverage of the antitrust laws and the desire in some cases to reach for more certainty in the legal environment.

An antitrust exemption limited in scope is needed to address the prospective, hypothetical nature of the problem faced by private sector companies and groups engaged in critical infrastructure information sharing. Other procedures – notably the Business Review Letters of the Department of Justice Antitrust Division – can provide some benefits by ratifying that establishment of formal procedures is without antitrust risk, but that alone is not enough to encourage the kind of information sharing that should take place in an unplanned, informal crisis environment. The Business Review Letter procedure, while well suited to consideration of ordinary commercial ventures, falls short when it is applied to the extraordinary demands of critical infrastructure information sharing.

Any time competitors come together for a joint project of some sort – for example as an ISAC[1], a trade association, or a consortium to implement the recovery from an attack on critical infrastructure – antitrust counsel immediately focus on questions of the elevated risks of such enterprises. The risks are inherently higher than for other groups because competitors can be found liable under the antitrust laws if they engage in certain conduct – without ever having to prove that the conduct itself has anticompetitive effects. Those effects are presumed – the violation is "per se" -- when "horizontal competitors" are acting in concert.

Of course, in the vast majority of cases, competitors meeting together for legitimate purposes scrupulously avoid the kind of conduct -- restricting output, influencing prices,

[1] Information Sharing and Analysis Center

dividing markets or otherwise inhibiting competition – that the antitrust laws address, but the risk is always there and is magnified somewhat by the ambiguity of the broad mandates of 100 years of antitrust jurisprudence.

Recognizing the need for greater certainty in the business community, the Antitrust Division of the Department of Justice has a procedure for issuing "Business Review Letters" (BRLs) that express the Department's enforcement intentions with regard to a particular proposed course of business conduct.[2] The question is whether this BRL policy and procedure is sufficient to meet the needs of the private sector engaged in the process of sharing critical infrastructure information for the purpose of preventing future incidents, strategic planning about vulnerabilities, or recovering from the effects of attacks or incidents that have already taken place. The answer is that while the BRL procedure may offer assistance in some cases, it cannot provide all of the additional measure of certainty that the information sharing process deserves. A narrowly crafted antitrust exemption can do a better, more extensive job.

Benefits of a BRL

1. A BRL gives a government imprimatur to a proposed course of conduct that does not in the first instance pose any antitrust risk. It should confirm counsel's advice and reassure a client concerned in light of the high risks that antitrust problems can entail.

2. While a BRL is in effect, participants in the covered activity have certainty that the conduct they are engaging in will not result in a lawsuit by the U.S. Department of Justice.

Limitations of a BRL

1. The Department cannot issue advisory opinions, so will not give BRLs in response to hypothetical situations (What if X happened? Would it be permissible to engage in Y conduct?). While a BRL might serve to address the concerns about a concrete factual situation such as the establishment of an ISAC, it cannot address real-time information exchanges in a crisis situation that has not yet happened. And it would hardly be practical to seek a BRL after a crisis in order for companies to communicate on crisis recovery.

2. All of the actors must be identified in a request for a BRL. Parties not identified cannot take advantage of the intentions set forth in the BRL. This is another limitation on flexibility in the face of crisis.

3. Similarly, the proposed course of conduct must be fully described in the request for a BRL; conduct engaged in outside the described scope is not covered by any BRL protection. This could be yet another limitation on flexibility, absent carefully broad drafting of the scope of proposed conduct, allowing for all

[2] The regulation is at 28 C.F.R. Sec. 50.6 (2001)

possible future contingencies, in which case the request might fall into the trap of the hypothetical question.

4. The request for a BRL and all supporting documentation must be supplied to the Department and placed on the public record for comment (subject to claims of FOIA exemption). Should it be necessary always to advertise critical infrastructure security vulnerabilities on the public record in return for consideration of some antitrust guidance?

5. The claims of FOIA exemption are subject to the same limitations generally recognized regarding the so called "(b)(4)" exemption for business confidential information; limitations sought to be corrected by pending legislation. Moreover, the requestor subjects itself to the fact that the Department retains the right to keep the documents submitted in connection with a BRL and use them for "all governmental purposes." Confidentiality and limited use cannot be assured.

6. The BRL on its face states only the Department's current enforcement intentions and reminds the recipient that the Department remains free to change its mind at any time. At best, the Department suggests a commitment not to institute a criminal antitrust investigation, but civil action remains a possibility. This lack of certainty causes some antitrust practitioners to recommend against BRLs in most circumstances.

7. In fact, counsel must be sure that there is absolutely no antitrust risk BEFORE applying for a BRL. If there is any risk in the proposed behavior, and that behavior is disclosed to the Department, the Department may not simply decline to issue a BRL, but it may state its intention to commence an investigation. And it will have been supplied the data in the BRL application that it needs to go forward, at least on a preliminary basis. This is another reason antitrust practitioners often recommend against a BRL: If there is no risk, a BRL is not necessary; if there is some risk, the Department will not issue one and may in fact commence an investigation. It is worth keeping in mind this basic fact of business review letters: They do not grant antitrust exemptions; they only express the Department's enforcement intentions within the framework of existing law.

In sum, the limitations vastly outweigh the benefits. A BRL may be an excellent way to ratify that a research and development or production joint venture, or the sales and marketing plan of a trade association of competitors offering joint services, or similar commercial ventures are without antitrust risk. In the arena of critical infrastructure information sharing, however, an antitrust exemption limited in time and scope is needed to address the prospective, hypothetical nature of the problem encountered by the private sector. While a BRL provides a benefit by ratifying that establishment of formal procedures through ISACs is without antitrust risk, that alone is not enough to encourage the kind of information sharing that should take place in a crisis environment.

Testimony of Alan Paller
Director of Research, The SANS Institute

Before the
Committee on Governmental Affairs
United States Senate
Hearing on
"Securing Our Infrastructure: Private/Public Information Sharing"
May 8, 2002

Introduction

Chairman Lieberman and Members of the Committee, thank you for inviting me to testify today on information sharing for improved security. I am deeply honored. My name is Alan Paller. I am Director of Research for the SANS Institute. SANS is the primary training organization for the technologists who battle every day to protect the computer systems and networks in the global infrastructure. SANS alumni, more than 28,000 in all, are the intrusion detection analysts, security managers, security auditors, firewall analysts, system and network administrators, incident handlers, forensic analysts, and law enforcement officers who are responsible for building, maintaining, and auditing their organizations' cyber defenses, fending off attackers, and, when attackers succeed, investigating the crime and tracking down the criminals. SANS sees itself as not only the provider of formal education and training but also as a source of continuing education to these technologists on the front-line of protecting our critical infrastructure. Each week, more than one hundred and fifty thousand individuals receive SANS *NewsBites* and SANS *Security Alert Consensus* to keep them up to date on new developments in information security and new threats. We see information sharing as an essential element of what we do.

These technologists, the computer security professionals, are the front-line warriors in a constant fight against cybercrime. Every day, they are forced to engage the criminals who seek to use the Internet for financial gain or to disrupt commerce and government. The prize to the winners is control of the systems that operate our economy and provide the essential services on which we all depend. In my testimony today, I hope to illuminate the chain of nine primary stages in the battle and the consequences of losing at each stage. Then I'll show how sharing of five specific types of information, both from industry to government and from government to industry, can affect the outcome of the battle – perhaps changing in some measure the balance of power between the attackers and the defenders.

The fight against cybercrime resembles an arms race where each time the defenders build a new wall, the attackers create new tools to scale the wall. What is particularly important in this analogy is that, unlike conventional warfare where deployment takes time and money and is quite visible, in the cyber world, when the attackers find a new weapon, they can attack millions of computers, and successfully infect hundreds of thousands, in a

few hours or days, and remain completely hidden. The Code Red attacks last summer were perfect examples as is the current scourge sweeping through the Internet – the Klez worm.

One important objective of any sharing activities, therefore, should be to shorten the time it takes for the defenders to respond to new attacks. That requires not only strong computer security technical skills but also sharing of knowledge among the "good guys and gals" that is at least as effective as the sharing that goes on among those who would do us harm. To help us understand the nature of the battle and how information sharing makes a difference, I have constructed a model that shows what we see as nine stages of the cyber battle.

Nine Stages in the Fight to Prevent Successful Cyber Attacks

Stage 1. *Finding the vulnerabilities.* In the first stage defenders and attackers search for new vulnerabilities (called "zero-day vulnerabilities") that can be used to gain control of a system, remotely. When the defenders lose, as they do many times each year, attackers have an open door to any vulnerable system. However, so far, attackers who discover new vulnerabilities seem to use them narrowly to attack specific enemies. If they used them widely, some intrusion detection analysts would likely discover the attacks and spread the alarm. Discovery and publication would immediately shift the battle to other areas and tend to reduce the effectiveness of the attacks over time.

The most common examples of this type of vulnerability are called buffer overflows that are usually caused by programmers who did not check their programs for errors before releasing them to the public. A buffer overflow allows an attacker to send a command to a machine that does not belong to him, and force the machine to execute the command.

Five types of organizations and people are actively engaged in the process of finding and closing new vulnerabilities:
(1) The software development companies that create vulnerable systems test them; some hire outside hackers to test them, as well.
(2) Customers who deploy systems, especially those in major organizations engaged in electronic commerce, often hire penetration testing firms to try to "think like hackers" and find ways to compromise the security of their systems.
(3) Independent security researchers vie for the notoriety of being the first to point out a vulnerability.
(4) Military cyber researchers and their contractors search for vulnerabilities to be used either for offensive or defensive information warfare purposes.
(5) The criminals and their supporters search for vulnerabilities to exploit.

Stage 2. *Creating patches* The second stage begins when a critical vulnerability is discovered and made known to the system vendor. System vendors try to create and post patches to their systems before the hacker community posts attack scripts that anyone can

use to exploit the vulnerability. Once those attack scripts are released, the number and impact of damaging attacks quickly mount. The vendors often win this stage, but their users lose anyway because they don't win the next battle.

Stage 3. *Distributing and installing patches* Once a patch is available for a critical vulnerability, the third stage begins. It is the race to protect large numbers of systems by persuading system administrators to install patches before attackers launch automated programs that scan the Internet for unpatched systems or systematically attack all e-commerce sites (or others groups of interest) looking for systems that have not been patched. There is ample evidence – the Code Red and Nimda worms are examples – that hundreds of thousands of Windows systems were still unprotected more than a month after a critical vulnerability was found, a patch built and posted, and announcements made that the patch needed to be applied immediately. That means that worms and other automated programs can take advantage of these vulnerable systems long after the vendor has released a patch.

Stage 4. *Finding and stopping worms.* During the past fourteen months, a series of worms have spread through the Internet. Worms use recently discovered vulnerabilities to take control of vulnerable systems. A worm as we use the term in cyber security, is a particularly insidious form of parasite that not only infects the machine that it has attacked, but also immediately puts every new victim system to work searching for more victims. That's why worms like Code Red and Nimda spread so fast. Worms can exploit hundreds of thousands of systems in just a few days. Some worms do a great deal of damage. The Lion worm (March 2001) stole thousands of password files and sent them to China.com. Once a password file has been stolen and cracked, every account on that system (and on other connected systems where the same account names and passwords are used) is open to exploitation. So when a worm is launched, the fourth stage begins. In this battle, the defenders try to find new worms that have been unleashed on the Internet and block their most damaging impacts before all vulnerable systems have been exploited.

This is an area in which a private/public partnership has emerged and prospered. SANS operates the Internet Storm Center. It collects data from hundreds of sensors around the world and has been able to put out early warnings of new worms spreading on the Internet. Immediately upon discovering any indication that a worm is loose, SANS informs law enforcement and DoD personnel as well as a council of very smart security practitioners around the globe who have proven capable of breaking these worms. Storm Center was responsible for finding both the Lion and Leaves worms last year. In the case of Leaves, which had taken over more than 20,000 systems and had complete control of them, Dick Clarke's staff at the White House and officials of the National Infrastructure Protection Center convened a joint public/private technical response team and together they broke the code of the worm and caught the criminal who had started it.

Stage 5. *Updating minimum security benchmarks.* Months, even years after vulnerabilities have been discovered and patches have been posted, huge numbers of people continue to connect unpatched systems to the Internet, so the fifth battle is to establish consensus agreement on minimum benchmarks for safe configurations that can

help every user know what needs to be done to use their systems safely. This stage is important and it is often misunderstood. What we are talking about here is the equivalent of standards for aircraft maintenance and configuration. If anyone ever sits before this Committee and tries to persuade you that it would be bad policy to set standards for securing information systems, I hope you will ask them whether they also think it is bad policy to set standards for configuration and maintenance of passenger aircraft. Without standards for secure configuration, only the most security-savvy users have the knowledge needed to keep their systems safe. With standards, users can not only buy systems that are well protected but also automate the process of keeping them protected. Time is of the essence here. Every day additional applications are being developed using unsafe configurations. When agencies or companies buy such unsafe applications, they often have to reduce the security settings on their current systems to install and use the applications, obviously a backward step in security.

Before going on to describe the next stage, I would like to take a moment to tell you about an important public/private partnership and the work it has done. The National Security Agency and the National Institutes of Standards and Technology, in cooperation with the Center for Internet Security and the SANS Institute, with substantial help from Microsoft, have reached initial agreement on a benchmark for securing Windows 2000 computers – by far the most popular type of system being deployed as servers in government and in the commercial world. Their joint action will lead to testing of applications to be sure they work correctly on securely configured systems and do not force users to reduce security. Their effort will lead to automation of security configuration and testing, and it will lead to procurement language that allows federal agencies and commercial organizations to order securely configured versions of Windows 2000. The group is also making rapid progress on security benchmarks for Cisco systems and Sun Solaris systems. Benchmarks for several other operating systems are in the pipeline.

Stage 6. *Finding victims and fixing their systems.* The sixth stage happens because attackers do not use their own systems for the majority of attacks. Instead they take over other people's vulnerable systems and use those victim systems to scan for additional victims. In this stage, the defenders try to find exploited and infected machines and persuade their owners to fix them, before those systems exploit more victims and before they are used by attackers in large scale, distributed denial of service attacks. This race should be easy for the defenders to win because networks of sensors in the Internet Storm Center and at UUNET and other organizations are constantly identifying systems being used in attacks. However, when the Internet service providers (ISPs) that connect these attacking systems to the Internet are informed of the problem, many of them ignore the warnings. Government and the private sector could do more to solve this problem by working together to raise the visibility of the systems being used for broad based attacks.

Stage 7. *Deflecting or stopping distributed denial of service (DDoS) attacks.* In the seventh stage, victims being subjected to distributed denial of service attacks try to get the attack stopped before their business deteriorates irretrievably. Innovations by UUNET (WorldCom) have helped improve the defenders' chances, but for many types of

DDoS attacks, there is little the defenders can do other than wait until the attackers tire of the game.

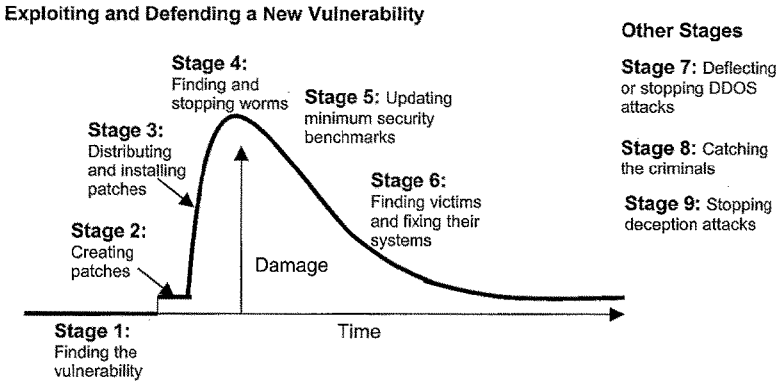
Stage 8. *Catching the criminals.* In the eighth stage, law enforcement people work with technical experts from the victim organizations and other helpers to track down the successful hackers before they do more damage. Of all the stages of the battle, this is the one that should make us all feel pretty good. The FBI has done an extraordinary job of tracking down cyber criminals and deserves our great appreciation for increasing the risk faced by attackers. I would prefer to prevent attacks, but some will always succeed. It is gratifying to see the international cooperation and deep technical expertise the FBI has developed paying off in convictions.

Stage 9. *Stopping deception attacks.* While the defenders are trying to block attackers who probe and exploit vulnerabilities in the systems and software, other attackers are making a mockery of the defenses by persuading gullible users to open up back doors that allow attackers to control systems inside the otherwise secure perimeter. They send an instant message or forge an email or create a web site that persuades users to download and run programs. The programs seem helpful – some even masquerade as "critical" security patches - but when the user executes the downloaded program, it installs a back door and, more recently, opens a connection through the firewall to another system controlled by the attacker. And once the attacker controls one trusted system, he can often gain control of many other systems inside the organization. The ninth stage, then, is to get the users educated so they know how attackers get in and what to do to stop them, before the attackers take advantage of their naiveté.

And in the spirit with which this hearing is being called, to help protect the infrastructure, I should add that security awareness is an important undertaking for every user organization. If someone wanted to take control of the computers Senate staff members use to conduct business with each other or to interact with the press or key constituents, they would most likely use one of the approaches I outlined in stage 9, because deception attacks often elude computer-based cyber defenses.

Chart 1, below, illustrates how the nine stages in the battle correspond with first a rise and later a fall in the damage attackers can cause using a new vulnerability. As the chart tries to make clear, catching attacks at the earlier stages will significantly reduce the damage that they do.

Chart 1: Cyber Attack Stages



Let's move on to information sharing that can help the defenders win more of those battles.

How Information Sharing Can Help Defenders Protect the Infrastructure

Sharing five types of information can help win the war against attackers.

Type I. Data on vulnerabilities and information technology assets with potential vulnerabilities.

This type covers two sets of information: the inventory of information technology assets and the actual vulnerabilities found in that inventory. Inventory data is of particular interest in critical infrastructures such as power production and distribution, telecommunications, and air traffic control, because some of the key systems used in those sectors are unique to each sector and are often found throughout the sector. If a major threat to one of those shared technologies is discovered, how can you protect the infrastructure in that sector if you do not know where in that sector the vulnerable technology is being used? Sharing inventory data helps the defenders distribute and deploy security patches quickly (Stage 3).

Another opportunity for sharing arises when one organization finds vulnerability in a key system. The vendor that built that system may not act immediately to create a patch (Stage 2). If the user can share the discovery with other users and government, these

groups can act together to bring substantial additional pressure to bear on the vendor to produce a new patch. We saw a great example of this during the SNMP threat late last fall when ISPs and government acted together, but outside the public view, to pressure router vendors to develop a patch that protected their customers from the single packet denial of service attack made possible by the SNMP vulnerability.

A third opportunity for sharing data on vulnerabilities is one in which the US General Services Administration has made enormous progress. GSA recently established a single common source of information for all federal agencies answering three key questions: (1) What new vulnerabilities have been discovered? (2) How much control can an attacker gain and how easy is it for an attacker to exploit each new vulnerability? and (3) Where can the user find the patch that corrects each of them? The GSA service will launch June 24th. It would be wonderful if this free distribution were not limited to the Federal government. Just as the federally funded National Weather Service provides information to all citizens on severity of hurricanes, so federal sharing of information about the criticality of new computer security vulnerabilities could help all users of vulnerable computers. For now, however, GSA's offering is the best we have seen. This type of sharing is a great help in distributing and installing security patches (Stage 3) and forms much of the basis for updating minimum security benchmarks (Stage 5), as well.

Just knowing that vulnerabilities exist is not entirely sufficient. To craft an appropriate national response to a major threat, one also needs to know that a vulnerability is being actively exploited. For that you need some or all of the next three categories of data

Type II. Data on attempted (unsuccessful) attacks

Millions of unwanted communications hit large companies and government agencies every day, and their firewalls and screening routers block nearly all of them. The unwanted data is being sent by hackers and by programs the hackers launch or by incorrectly configured systems somewhere on the network. Hidden in that flow of bits across the Internet is information that can tell us a new worm has been launched, and as I mentioned before, Storm Center – a cooperative effort among private and public organizations – is already and sharing this data. Storm Center has discovered two major worms and helped stop their damage in one case and led to the arrest of the hacker in the second. The Center is a free public service, and many companies willingly send the data from their firewalls to Storm Center, in part because the Center enables them to remove identifying data from their submissions. Storm Center can be much better than it is and we are investing heavily to improve its precision and speed.

Sharing data on attempted but unsuccessful attacks helps in two ways. First, it helps find and stop worms (Stage 4). Second, it helps find systems that have already been exploited and are being used in untargeted attacks (Stage 6).

However, Storm Center's sensors are far too sparsely distributed in Internet space to find attacks focusing on specific industries or critical sectors such as telecommunications or electric power. For this service to be helpful in more targeted attacks, Storm Center

would need to be replicated in each sector. To encourage that type of sharing, SANS has offered to make the Storm Center software available at no cost to any Information Sharing and Analysis Center (ISAC)* that wants to have a public or private collection and analysis system.

Although data on unsuccessful attacks is extremely useful in illuminating broad attacks such as worms, it is not the answer for rapid response to targeted attacks on the infrastructure. For that you need data in the next category.

Type III. Data on successful attacks as they are first discovered.

Data on successful attacks as they are happening is likely to be the most valuable information that can be shared and could help enormously in distributing and deploying security patches (Stage 3), updating minimum security benchmarks (Stage 5) and catching the criminals (Stage 8). Rapid sharing of information on ongoing attacks could improve the chances that organizations most likely to be the next target would act quickly to defend themselves and even set up honey pots to help catch the culprits. Sadly this data is the least likely to be shared. Anecdotal evidence suggests that those who have been attacked successfully are reluctant to share information about the attack – or even admit that they were attacked – for two reasons. They fear that public disclosure could embarrass the organization and possibly cause their customers to abandon them. That's a "bet your company" risk. Further, the experience of the ISACs shows that when an organization is under attack, its technical employees are so busy that they don't even think of telling anyone outside about the problem – unless they want help from consultants in cleaning up or help from law enforcement to catch the culprits.

Those last exceptions – where companies want help from consultants or law enforcement people -- offer two small windows through which real-time attack data can be shared. When the organization that runs the ISAC also contracts with individual ISAC members to provide rapid response forensics and clean-up services when those members are being attacked, the ISAC can be an extremely effective means of getting patches installed quickly (Stage 3). Law enforcement can also offer valuable information on actual attacks, and I'll talk about that in the discussion of the final type of information.

Discussion with officials at the General Services Administration, which operates the Federal Computer Incident Response Center (FedCIRC)**, suggest that Federal agencies are equally unlikely to report incidents very rapidly for the same reasons, fear of embarrassment and preoccupation with dealing with the immediate problem.

---

* ISACs have been established in financial services, information technology, energy, telecommunications, and electrical utilities, and others are under development. They are private organizations that promote the exchange of information on security threats and breaches among their members.

** FEDCIRC is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government (www.fedcirc.gov).

Type IV. Analyses of the cause and impact of attacks

When attacks are understood and information about how they were conducted is shared, organizations focus on eliminating the risk because both their senior managers and technicians know the risk is real and know how to avoid it. Thus sharing attack analyses can help in distributing and deploying security patches (Stage 3), updating minimum security benchmarks (Stage 5) and, when the attack involves taking advantage of overly trusting users, can also help with stopping deception attacks (Stage 9).

Companies are just as reluctant after the attack as they are during the attack, to take the chance that information about their security breach would be made public. They act as if experiencing a security breach is similar to contracting a social disease.

Sharing after-attack analysis data is an area in which consultants and law enforcement can and have helped. Consultants and law enforcement agencies can be filters that pass data to other potential victims without identifying the current victims. A great example of the value of this type of sharing took place last spring when the FBI's National Infrastructure Protection Center revealed that organized crime groups were targeting ecommerce and ebanking companies for extortion. The criminals systematically exploited a pair of web server vulnerabilities in hundreds of ecommerce companies, stealing credit card information and other private customer data. Then they threatened the e-commerce companies saying they would publish the private customer information on the Internet if the company did not pay 100,000 Pounds Sterling. Although the FBI had many ongoing cases, and disclosure could have compromised the investigations, the NIPC told the world about the crimes and exactly which vulnerabilities were being exploited. Their announcement persuaded many e-commerce and e-banking organizations to act quickly to protect themselves, and told them exactly how to do it.. More sharing of that nature could do a great deal of good in Stage 3.

Type V: Safe Configuration Benchmarks

Safe configuration benchmarks are the synthesis of data from the other four categories. They bring together knowledge about vulnerabilities, successful and unsuccessful attacks, and the best methods to block attacks. Few organizations are large enough or have sufficient access to private law enforcement information to build effective configuration benchmarks alone. They lack a complete picture of the risks they face and the actions they should take to eliminate those risks. On the other hand, many experts believe that more than 80% of the successful attacks of the past two years could have been stopped if the organizations had taken specific minimum steps to secure their systems. Therefore, one area of great opportunity to prevent attacks, thereby helping win several stages of the cyber security war, is to share a set of minimum benchmarks for securing common operating systems.

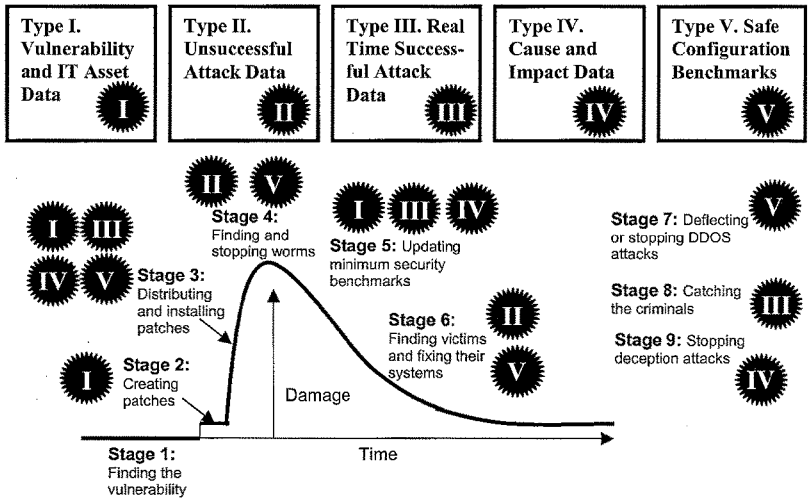
The initiative I spoke about earlier is central to this sharing effort. NIST, NSA and the Center for Internet Security came to agreement on a benchmark for securing Windows 2000 and are nearing agreement on other popular systems. Once these benchmarks are

shared, and tools are available to test systems, four stages in the battle will be much easier for defenders to win: stage 3 (distributing patches), stage 4 (stopping worms), stage 6 (getting infected systems fixed – because there will be fewer of them), and stage 7 (stopping DDoS attacks because there will be fewer victims to use for DDoS).

If this Committee can help ensure that federal agencies use their purchasing power to acquire safer systems from the vendors using the consensus benchmarks, you will have an enormous effect on federal cyber security. In addition, the private sector will quickly follow the federal leadership. One easy way to encourage such action would be to add to the reauthorization of your Government Information Security Reform Act, a few words requiring federal agencies to report to NIST or OMB the specific configuration benchmarks they are using to test security of the systems they are deploying.

The chart below illustrates the stages of the battle that can be helped by sharing each type of data.

Information Sharing Can Help In All Stages



Conclusions on Information Sharing

As the Internet grows in importance over time, Internet security will increasingly coincide with economic security. But computer security is hard, and it is made even harder when each user must act alone because he doesn't have access to critical information from other users. You can help in four ways: (1) by removing barriers that keep the private sector from sharing data with government, (2) by encouraging the federal government to share data it has on vulnerabilities and attacks with the private sector, (3) by requiring federal agencies to lead by example by testing all their systems against security benchmarks, and (4) by asking that all newly acquired federal systems meet minimum security benchmarks except where such a requirement would disable a mission-critical system.

Mr. Chairman, I hope that this framework is helpful as the Committee examines the important role that timely sharing of information plays in preventing, detecting, and recovering from cyber attacks. Clearly, greater and timelier sharing of all of the types of information outlined above can significantly reduce the damage being done by those who would exploit our technology infrastructure whether for financial gain or to terrorize us. The impediments to sharing, some of which I have enumerated above, are complex. One alleged impediment, which I am not able to evaluate, is a concern that, in reporting to government, companies will give up control over proprietary information and that such information might ultimately even be made public. In that regard, it is interesting to note the experience of private ISACs, where no such threat exists, who report similar problems with under-reporting. If a case is made for broader guarantees of confidentiality, and existing restrictions for certain national security, trade secret or law enforcement information are deemed to be insufficient, I would urge the Committee to draw any new restriction on public access as narrowly as possible by defining the categories of information that would be kept confidential quite precisely. To do otherwise, could very well create a new impediment to the sharing of cyber security information so vital in the war we are waging where the government might be unable to pass warnings along because of FOIA restrictions. The enemy - and make no mistake about it -- he or she is an enemy – uses the Internet to great effect to share information. We need to be at least as effective.

We at the SANS Institute and, I believe, the entire community of SANS alumni, will continue to work every day to do our part to turn the tide against cyber attacks.

Thank you very much for this opportunity to share my views with the Committee, and I look forward to your questions.

STATEMENT OF
TY R. SAGALOW

BOARD MEMBER, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS ISAC)

CHIEF OPERATING OFFICER, AIG EBUSINESS RISK SOLUTIONS

MAY 8, 2002

Mr. Chairman and Members of the Committee, thank you for this opportunity to testify about the importance of information sharing in the protection of this nation's critical infrastructure. My name is Ty R. Sagalow and I come before you in two capacities today. First, as a member of the board of the Financial Services Information Sharing and Analysis Center – the FS ISAC—FS ISAC is the oldest Information Sharing and Analysis Center established as a result of Presidential Decision Directive 63, and secondly as the COO of American International Group's eBusiness Risk Solutions division, the largest provider of network security insurance in the world.

Governor Tom Ridge recently remarked:

> Information Technology pervades all aspects of our daily lives, of our national lives…Disrupt it, destroy it or shut down the information networks, and you shut down America as we know it.

The sad fact is that our information technology systems are already under attack and there is every reason to believe it will get worse before it gets better. According to a recent report of the National Research Council, U.S. companies spent $12.3 billion to clean up damages from computer viruses in 2001. Further, the report notes that 2002 could be worse. The 2002 CSI/FBI survey found that 90% of companies surveyed admitted to a successful computer breach in the preceding year resulting in hundreds of millions of dollars in quantifiable losses. Mass cyber-events such as "I Love You" virus, the Mellisa Virus and more recently Code Red and the NIMDA viruses are reported to have caused hundreds of millions, perhaps billions, of dollars in damages. Finally, the CERT organization at Carnegie Mellon reports that in 2001 they received over 50,000 incident reports, more than double of the year before which itself was double of the prior year.

Today, it would be easier for a cyber-terrorist to shut down a dam by hacking into its control and command computer network than to obtain and deliver the tons of explosives needed to blow it up. More frightening, the destruction can be launched from the safety of the terrorist's living room couch – or cave as the case may be.

We must act and we must act quickly. Fortunately, we are not powerless. Just as it is our information systems that are the subject of the attacks, it is our ability to share information which provides our best foundation for defense.

In October 1997, the *Report of the President's Commission on Critical Infrastructure Protection* identified the banking and finance sector as critical to the nation's well being. This finding was incorporated in PDD-63 in May 1998 and on October 1, 1999 at the request of the US Department of Treasury, the Financial Services Information Sharing and Analysis Center was born. Today there are over 53 financial institutions representing more than 50% of all credit assets who are members of the FS ISAC. Members include 5 of the top 10 commercial banks and 5 of the top 10 securities firms, as well as numerous insurance companies such as AIG.

The mission of the FS ISAC is straightforward: Through information sharing and analysis provide its members with early notification of computer vulnerabilities and attacks, subject matter expertise and other relevant information such as trending analysis.

We are joined in this endeavor by other organizations with similar missions. One of these is Infragard which as you know works with the National Infrastructure Protection Center (NIPC) and the private sector to create a trusted network of information sharing.

Unfortunately, I am here today to tell you that we will not succeed, we cannot succeed, in this mission without your help. Existing laws and regulations today place severe obstacles preventing the voluntary disclosure of information from the private sector to the public sector and within the private sector itself.

We believe that there are chiefly three obstacles that must be removed for effective, robust information sharing to take place. Removing these obstacles is important since companies will not disclose voluntarily if their general counsel tells them not to. And general counsels will tell them not to if there is a potential that disclosure will bring financial harm to their company. It is that simple.

As respects sharing information to the public sector, the fear exists that the competitors or others, wishing to do the disclosing company harm, will be able to obtain access to that information through the Freedom of Information Act. As respects sharing information within the private sector, there are two twin fears. First, such sharing could be deemed to be violation of either federal or state anti-trust laws and second, that the sharing of information will lead to liability against the company or its directors or officers.

The chilling effect of potential liability lawsuits on voluntary speech cannot be underestimated. Private lawsuits, or rather the fear of them, have always played an important role in fostering proper conduct. However, when applied inappropriately, they can have the opposite impact – that of chilling desirable conduct. Such is the situation here. Why disclose the potential inadequacies of a security technology when your general counsel tells you that the disclosure could lead to a defamation suit? Why recommend the use of specific technological safeguards when such disclosures could lead to lawsuits alleging tortuous interference with the contractual rights of others who

use competing technology. Why freely disclose the results of millions of dollars in research and analysis of "best practices" when such disclosure could lead to shareholder lawsuits alleging misconduct in disclosing company "trade secrets" or other breaches of the fiduciary duties.

"The risk is too great." "Better to keep your mouth shut." "Better safe than sorry." These statements represent the danger that we face today fore that will be the advice given by general counsels throughout the nation. We faced this danger before, in Y2k and in Y2k we avoided it through thoughtful and balanced legislation. We must avoid the danger again.

Putting on my other hat, I can tell you that information sharing is essential to the creation of a stable insurance market for network security. Insurance plays a critical role in protecting our national infrastructure by both spreading risk among members of society as well as providing positive reinforcement for good behavior by making insurance available and affordable. *BusinessWeek* recently remarked that it will be the insurance industry which over time will influence security software standards. A working insurance industry provides a vital mechanism to structure and reward security "best practices".

Today, my company leads the way in this effort and we have already provided billions of dollars in insurance protection for thousands of companies representing all segments of our nation's infrastructure. This is but a drop in the bucket, however. Today, there are only a handful of insurance companies providing network security insurance. The reason: insurance companies cannot underwrite what they do not understand. And they cannot understand a risk if they do not have access to data on frequency and severity of risk—or at least the hope of future access to such data. Effective and robust information sharing becomes the foundation for building the actuarial tables needed to create a stable insurance industry.

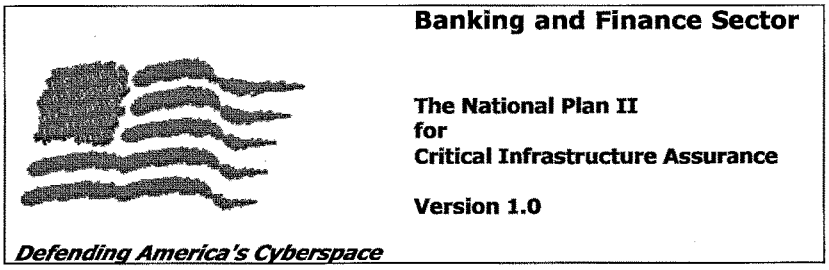
In conclusion, for voluntary information sharing to be both robust and effective, the Government should take three actions:

1. Provide an exemption under FOIA for critical infrastructure information voluntarily shared from private companies or private sharing groups to the federal government,

2. Provide an exemption or guidance under the anti-trust laws on both a federal and state level to critical infrastructure information voluntarily shared in good faith within the private sector, especially within a formal structure like the ISACs, and

3. Provide safe harbor legislation similar to that provided for Y2k to protect the disclosure of critical infrastructure information within the private sector as long as such disclosure is made in good faith.

Mr. Chairman, I would like to thank the Committee for permitting me to testify today on this important subject. I would be pleased to answer any questions you might have at this time.



B. Insurance Risk Management

Within the banking and finance sector, the insurance industry plays a critical role in protecting the nation's critical infrastructure from cyber risks. The industry is in the unique position to motivate positive risk management steps by rewarding such steps with the availability and affordability of insurance protection. Insurance carriers should be encouraged to create specific cyber risk insurance policies with terms and premium adjustable to the quality of the risk management of the insurance applicant. Insurance carriers should be encouraged to fulfill three basic obligations:

- Provide loss prevention or mitigation services through high-quality independent technology companies;
- Provide reasonable financial loss risk transfer in the event of a cyber attack or cyber-extortion attempt for a premium that is neither excessive nor inadequate for the risk: and
- Provide post-incident support.

Companies whose products or services directly or indirectly impact the economy or the health, welfare or safety of the public should be encouraged to purchase specific cyber risk insurance programs from financially strong insurance carriers.

Examples of loss prevention or mitigation services offered by insurance providers include security assessment services, whether online or, preferably, on-site as well as low-cost or free perimeter scans. The cost of these services should be incorporated into their insurance premium or preferably provided free of charge as a means of lowering risk. Insurance carriers should be encouraged to develop strategic alliances with technology companies providing risk reduction products and services for which carriers might discount the premium of their insurance policies as further motivation to insurance applicants to utilize best-in-breed security.

To maximize effectiveness, insurance carriers should be encouraged to provide broad financial risk loss transfer insurance directed toward cushioning the financial impact of litigation, loss of Internet revenue (due to denial of service attacks), and damage to data for companies that have demonstrated that they have incorporated reasonable risk management techniques in the handling of their cyber-risk exposures.

The security of the nation's critical infrastructure cannot be obtained without active involvement of a company's board of directors. Directors should take an active role in the management of cyber risk just as they took an active role in the management of the Y2K crisis. Director and Officers (D&O) insurers should be encouraged to assist in the education of boards and, when appropriate, modify applicable terms and premium of their D&O policies consistent with the level of the board's management of this area.

Since public confidence is cornerstone of the nation's economic viability, insurance carriers should be encouraged to support enhanced long-term stability by providing post-incident support funds. Examples of such funds would include crisis communication services geared toward restoring confidence in consumers, employees, shareholders and other stakeholders of the insured company.

There are insufficient funds in the insurance industry to transfer the financial loss of mass cyber-events. As a result, the banking and finance sector recommends that the public sector address the issues associated with catastrophic cyber reinsurance programs.

[Note: the following two paragraphs may appear moved elsewhere in the report and are reproduced here for simplicity.]

Congress should be encouraged to pass laws necessary for this purpose and the Executive Branch should be encouraged to issue regulations based on existing laws to achieve this purpose to the extent possible. In addition to mass cyber-events such a program would be used for risks uniquely applicable to public sector concern such as cyber-war and cyber-terrorism.

Information sharing between the public and private sector and within the private sector is essential to the security of the nation's critical infrastructure. Robust information sharing will not occur unless the legal and economic obstacles preventing such sharing are removed. These obstacles include the potential application of FOIA to information shared with the public sector, the potential for application of federal and state antitrust laws to information shared among private sector companies and the potential for legal liability arising out of the disclosed information as well as the decision to disclose. Lessons from legislation enacted for Y2k disclosures are especially useful. Accordingly, Congress should be encouraged to pass disclosure laws on FOIA, Antitrust and liability similar to those passed for Y2k.

Spend some quality time with your money. BusinessWeek tv MONEYTALKS

APRIL 2, 2002

SECURITY NET
By Alex Salkever

E-Insurance for the Digital Age

Big insurers are now offering policies against hacks, viruses, and stolen data. They may also set security standards

The past six months have been tough on the insurance industry. Claims resulting from the September 11 terrorist attacks have totaled into the tens of billions of dollars. At the same time, insurers are struggling to recover from a decade of price wars that left reserves depleted. But one tiny part of this sector is going great guns -- the e-business insurance market.

This broad rubric covers policies that address threats new to the Digital Age, including virus attacks, denial-of-service assaults, cracking into company systems, and Web-site defacements. Some companies even write policies that cover cyber-extortion, where an online intruder or an insider steals crucial data such as customer credit-card files and demands a payoff. The rising tide of lawsuits against companies whose employees have used corporate e-mail inappropriately has also caught the attention of e-insurers.

The repercussions could be sweeping. Why? Because insurers will probably become a major force in shaping the computer- and network-security business. They'll likely mandate what types of security practices, providers, and products are acceptable, just as they've shaped practices and products in the construction and auto industries. "Things like CodeRed [a computer worm that appeared in July, 2001] are happening so often now that cyber-insurance will become ubiquitous. Then [insurance] price differentials will appear for different types of software," says Bruce Schneier, chief technology officer of Counterpane Internet Security.

BILLION-DOLLAR BUSINESS. From a standing start two years ago, revenues from policy purchases grew to just shy of $100 million in 2001, according to insurance execs. "This will be at least a $1 billion market by 2007," says Ty Sagalow, chief operating officer of American International Group's eBusiness Risk Solutions Group.

He should know: AIG (AIG) holds approximately 70% of the global e-insurance market and has written 1,500 policies for companies ranging in size from small businesses to giant corporations. AIG is best positioned to influence security software standards, and it's already doing so.

Other major players such as Chubb (CB) and Zurich North America (ZFSVY) now offer their own policies. Such coverage isn't cheap: A typical policy costs hundreds of thousands of dollars annually for only tens of millions of dollars worth of coverage. But these policies could become a mandatory

cost of doing business in the next five years.

APPROVED SOFTWARE. Security experts point out that in the past few months several insurers, including AIG, have rewritten some of their general business coverage to specifically exclude cyber-hazards. "I would make an argument that most of them never did intend to cover it. They have just clarified matters," says John Wurzler, vice-president for worldwide sales at cyber-insurance broker Safeonline. Plus, two recent court cases have upheld insurance companies' claims that standard business policies don't cover damage to data and other nontangible business assets.

These developments set the stage for insurers to begin setting de facto security standards for customers. As part of AIG's NetAdvantage policies, it offers customers a 10% discount on security software from Computer Associates (CA), according to AIG's Sagalow. "What we prefer to do is look at a piece of software and believe that if it lowers the risk for our insurance, we make it available to them," he says.

AIG has also partnered with managed security-services company RIPTech. Zurich Financial Services Group customers are encouraged to work with the insurer's managed security-services partner, TruSecure. And according to Counterpane's Schneier, his customers can get much lower rates on cyber-insurance from underwriter Lloyd's.

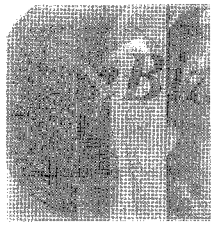
RISING PRESSURE. The same cost incentives can be extended to other services, such as data hosting. Witness the deal big insurance broker Marsh McLennan (MMC) struck in July, 2001, with communications giant AT&T (T). Companies that use AT&T's Internet data centers and managed Web-hosting services get a discount on e-business insurance from Marsh, as well as streamlined policy approval.

That's the wave of the future, as insurers exert even more pressure on the technology practices of any company wishing to insure this increasingly important facet of business. Schneier, for one, thinks that insurers will demand responsibility from software companies for flaws in their products -- and that they'll have the legal firepower to hold the software outfits accountable.

For now, insurers are more concerned with existing practices than they are about demanding specific software packages, say industry execs. And only a small percentage of companies have invested in cyber-insurance to date, by some estimates, less than 20%. Many still don't see the need for this type of coverage. "It's much cheaper to buy business-income insurance that can cover when there's a fire than it is to buy business-interruption insurance to cover when there's a hack," says Mike Zeldes, head of the cyber-insurance division of Kaye Insurance Associates, part of Hub Group.

As cyber-insurance goes from exotica to a business necessity, the computer-security industry will have to adapt to keep the insurers happy. That's good news for customers, since it will not only allow them to manage their cyber-risk but also give them a strong advocate for more secure software and hardware. The question is: How far are they willing to open their wallets?

Salkever covers computer security issues weekly in his Security Net column, only on BusinessWeek Online
Edited by Douglas Harbrecht



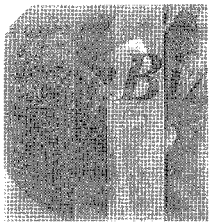
The Banking and Finance Sector

Critical Infrastructure Protection Initiatives

ISAC
INFORMATION SHARING
AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



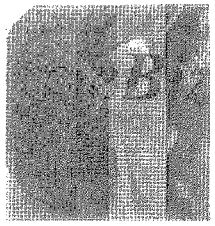
Agenda

- Background
- Objectives
- Initiatives
  - CIP Program
  - National Strategy
  - The ISAC
- Benefits
- Future
- Questions

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



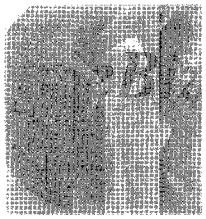
Background

- **May 1998 - Presidential Decision Directive (PDD) 63 was issued and:**
  - **Established goals for Critical Infrastructure Protection for the 8 Sectors**
  - **Recommended each sector protect itself from intentional acts which may diminish its capabilities**
  - **Requests implementation by May 2003**
- **March 1999 - Banking and Finance Sector PDD-63 Working Group sets goals:**
  - **Assure the viability and continuity of the Banking and Finance Sector**
  - **Ensure confidence in the ability to prevent, detect, and respond to incidents**
  - **Foster sharing of relevant information**

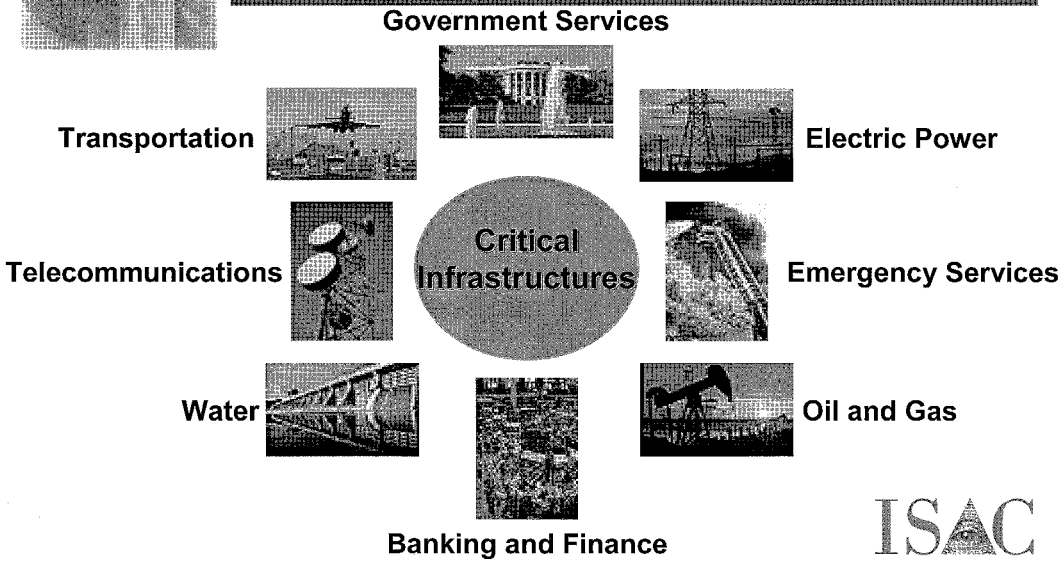
ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



U.S. Critical Infrastructures



ISAC
INFORMATION SHARING AND ANALYSIS CENTER

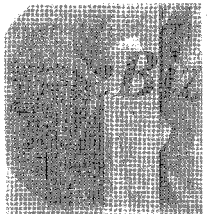
©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

Objectives

- Established the *Banking and Finance Sector Coordinating Committee on Critical Infrastructure Protection*
- Assumed responsibility for:
  - Assessing the vulnerabilities of the sector to cyber and physical attacks;
  - Recommending a plan to eliminate significant vulnerabilities;
  - Developing an information sharing system for identifying and preventing major attacks;
  - Proposing an agenda of research and development for information systems security;
  - Developing an education and outreach program to increase industry security awareness; and
  - Providing content for the industry's contribution to the *National Strategy.*

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

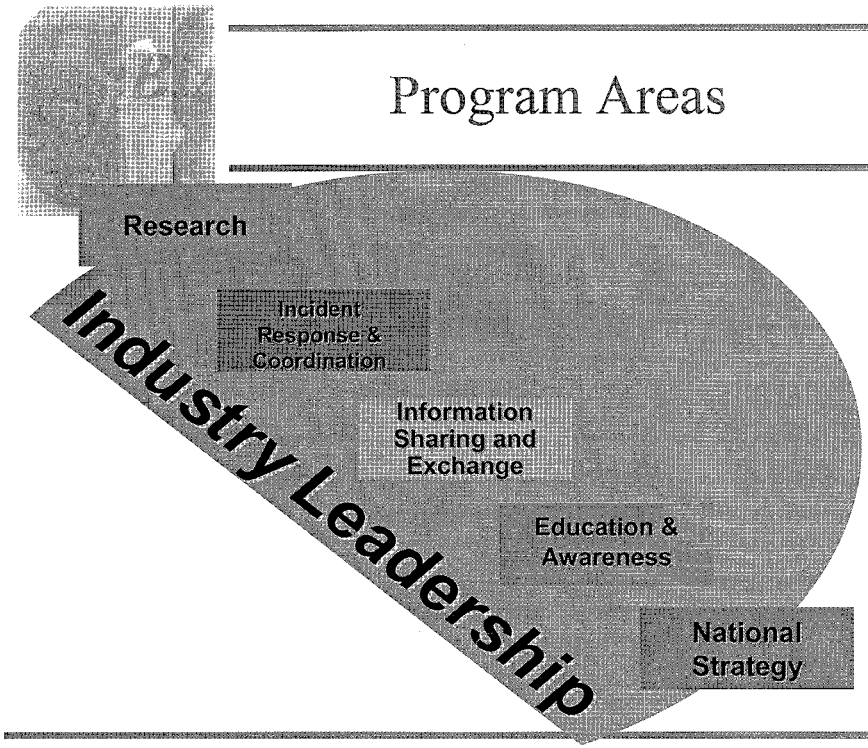


The CIP Program

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

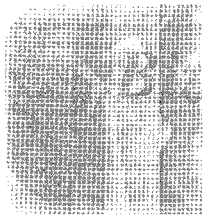
Program Areas



ISAC
INFORMATION SHARING AND ANALYSIS CENTER

7

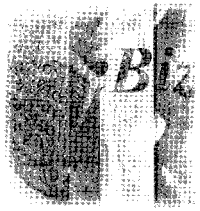
©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



Banking/Finance Sector CIP Coordinating Committee
Sector Liaison: Shiela Bair, Assistant Secretary - US Treasury
Sector Coordinator: Stash Jarocki, VP – Morgan Stanley

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



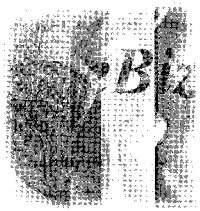
Guiding Principles

- The core infrastructure of the sector must be identified and assessed to determine potential vulnerabilities and exposures, which would pose systemic risk to the infrastructure.
- Owners and operators of the core infrastructure must be subject to a similar, consistent level of infrastructure assurance standards and oversight;
- Owners and operators of the core infrastructure must mobilize to defend and protect each other; and
- The Federal Government must work with owners and operators of the core, including the mobilization and provision of national resources as necessary, to defend, respond and protect the core infrastructure.

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



Key Assumptions

- Public/private partnerships are essential to meet challenges posed by new technologies and non-traditional threats;
- 20th-century government command-control policy frameworks and attitudes toward industry cooperation need to be adapted and modified to facilitate this partnership; and
- Both the public and the private sectors have to walk a fine line in balancing security and public/commercial interests

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

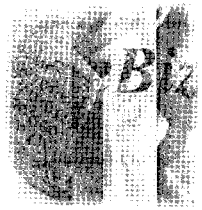
2002 FS-ISAC LLC Proprietary. All Rights Reserved

Key Initiatives

- Build and maintain the **Financial Services Information Sharing and Analysis Center (FS/ISAC).**
- Design, development and full operation of the **Financial Services Security Laboratory (BITS SECURITY LAB).**
- **Assess** the core institutions as a group to set a baseline for improving the infrastructure and identifying elements that could cause systemic failure.
- Develop a **Concerted Education and Awareness Campaign**.
- Establish a full **information exchange** program with all ISACs.
- Deliver the **National Strategy for Critical Infrastructure Assurance**

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



Current Activities

- Identification of the core infrastructure – those institutions & services that would cause systemic failure if they were unable to operate at full or limited capacity.
- Develop, refine and distribute sound practices through relevant industry and professional associations.
- Encourage FS/ISAC membership to include all levels of financial institutions to help communicate threat and vulnerability impact and solutions.
- Establish of Treasury sponsored security clearances for key individuals from the sector to facilitate communications with Government intelligence and judicial agencies.
- Establish robust Sector wide communications and alert system.

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved

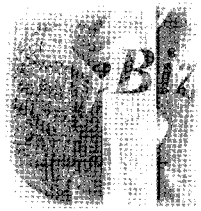
Activities (continued)

- Encourage the use of "LAB Tested or NIAP (National Information Assurance Partnership) Tested" products where available.
- Appropriate funds for the development and maintenance of an industry-wide simulation model of vulnerabilities for planning and reaction purposes.
- Perform semi-annual reviews of the infrastructure for newly developed weaknesses or threats based on new technology.
- Work with Treasury and other Government agencies to establish multilateral treaties to ensure consistent and usable torts and laws to assist in the protection of the infrastructure.

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary. All Rights Reserved



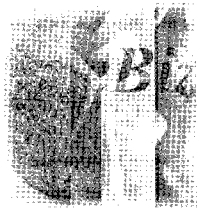
Financial Services Information Sharing Analysis Center, LLC

Cooperating to protect the Sector's Core Infrastructure

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

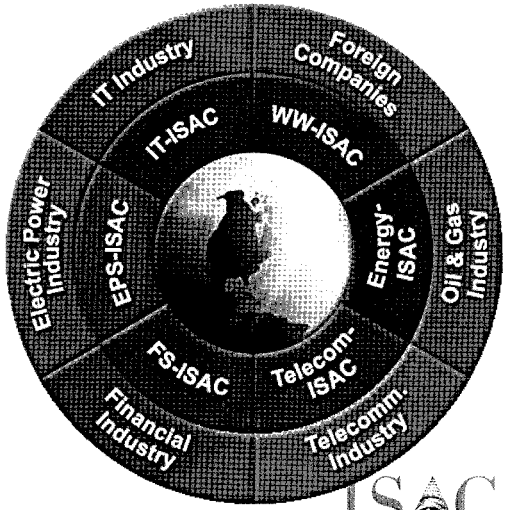
©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



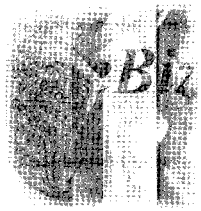
ISACs - Information Sharing and Analysis Centers

- Vital part of critical infrastructure protection (CIP)
- Gather, analyze, and disseminate information on security threats, vulnerabilities, incidents, countermeasures, and best practices
- Early and trusted advance notification of member threats and attacks
- Organized by industry: cross-sector awareness, outreach, response, and recovery



ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



The FS/ISAC

- The Banking and Finance Sector working group recommended the creation of a Financial Services Information Sharing and Analysis Center (FS/ISAC)
- The FS-ISAC, LLC was created to establish and govern the FS/ISAC for the financial services industry
  - Board of Managers of industry information professionals
  - Membership eligibility restricted to regulated financial services companies
- The FS-ISAC, LLC contracted with Global Integrity, a subsidiary of Predictive, to operate the FS/ISAC
- The FS/ISAC was launched on October 1, 1999 with pilot members and became fully operational in January 2000

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

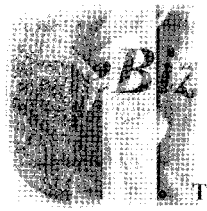
FS/ISAC, LLC Overview

- The FS/ISAC is:
  - A private sector partnership between eligible financial services providers
  - A database facility owned by the membership and facility managed by Global Integrity
  - An *anonymous* submission facility for security incidents and transmission system for alerts of serious incidents
  - A database structured to allow members to easily search for incidents, vulnerabilities, threats, and solutions
- Membership limited to:
  - FDIC insured banks
  - Licensed Insurance companies
  - Regulated industry utilities
  - NASD licensed investment firms
  - Specialized/regulated banking firms
- The FS/ISAC is available and operated 24 hours per day, 365 days per year

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



How the FS/ISAC Works

- The FS/ISAC offers members:
  - *Anonymous* or, if desired by the member, attributable incident submission
  - Multiple levels of incident analysis
  - Immediate notification of Crisis or Urgent alerts
  - Search capability on incidents, vulnerabilities, threats, and solutions
  - Portal configured for one stop provisioning
- FS/ISAC information sources include:
  - Member companies
  - US Government/law enforcement
  - Reliable private sector sources
  - Vendor Alliance members
- The FS/ISAC is exclusively for the use of member companies
  - No government or law enforcement agency will have access
  - Hosted in a secure, remote facility
  - Build with high reliability, high availability and security

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

© 2002 FS-ISAC LLC Proprietary, All Rights Reserved

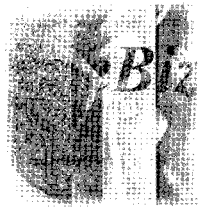
Historic Background

- 11/1/'99 – FS/ISAC is Launched
- 3/ '99 – FS/ISAC Working Group is born
- 3/ '00 – FS/ISAC revamps Database
- 2000 FS/ISAC warms members of Melissa
- 9/'00 – FS/ISAC holds first Annual Meeting
  - Membership grows to double digits
  - Global Integrity & FS/ISAC launch enhanced Database

- 12/'00 – Submit National Plan II for Critical Infrastructure Protection
- 2/'01 FS/ISAC early AK Virus warning beats the clock.
- 2/'01 Membership approaches 50
- 4/'01 – Mid-Year Networking Conclave
- 9/'01 – FS/ISAC Pulls out the stops to help members and non-members due to 9/11 and Nimda Crisis's
- 10/'01 – Second Annual Meeting
- 11/'01 – Portal Web Site Launch
- 12/'01 – National Strategy Issued

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary. All Rights Reserved



FS/ISAC Membership Profile
(January, 2002)

- Current FS/ISAC membership includes double digit organizations.
- Member organizations include insured depository institutions, securities firms, investment companies, insurance companies, credit card companies, government sponsored enterprises, clearing and settlement entities, and providers of financial technology.
- FS/ISAC members account for $$$:
  - Five of the top ten commercial banks
  - Five of the top ten securities firms
  - Over 40 percent of the total commercial bank assets, and
  - Over 40 percent of assets under management by the top 50 open end investment companies
  - Over 90 percent of assets held by financial service sector.

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary. All Rights Reserved

Virus Stats

- Love Bug
  - Beat the bug
  - Were prepared
- Melissa
  - Well versed in the technology
  - Cleaned our processors
  - Did not contribute to the problem
- Anna K.
  - Prepared and notified
  - No major member problems
- Nimda
  - First to alert members
  - Posted first solution set

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

Anna K. Virus Alerts

Alert Schedule:

10:53am McAfee

12:49pm ISAC member 1

1:47pm Symantec

2:05pm ISAC member 2

2:17pm ISAC alert (us)

7:51pm NIPC alert sent

11:54pm NIPC alert received*

From public sources (reasonably accurate). All times are EST Monday, Feb 12, 2001.
CERT alert sent Monday; time unknown / For other vendors, times unknown.
*(cause of delay unknown; could be our mail system)

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved

Information Sharing & Exchange

- USA vs. Global
- Working with other Sector ISACs
- Vendor Alliance
- Picking the right combination
- Working with Regulatory, Intelligence and Judicial Entities
  - Building Trust
  - Defining appropriate data elements to share
  - Building awareness

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved

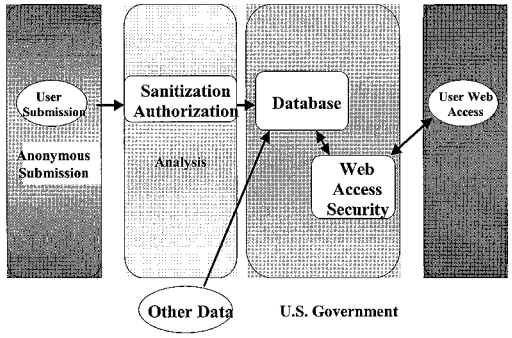
ISAC Functionality

Members:

- *May submit via anonymous, private, authenticated access*
- *Primarily web based with email back up*
- *Robust Search/Lookup capabilities*
- *Alerted to Urgent and Crisis events*

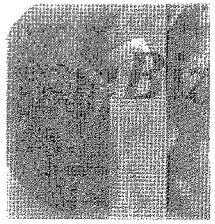
FS/ISAC

- *Analyzes each submission*
- *Automated and manual sanitization process*
- *Initiates alerts as defined by members*
- *Periodic trending and analysis*



ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



Facility Specifications

Facility

Physical Security

- *Remote, off-site*
- *24x7 Guarded Facility*

Environmental protections

Backup power

- *2 hour battery backup*

Network / Communications

- *Dual T-1s*

Computer / Network

Security

- *Lookup - SecurID*
- *Submission - SSL*

Backup

Disaster Recovery

Maintenance

Remote Security Monitoring

24 Hour Help Desk Support

Application

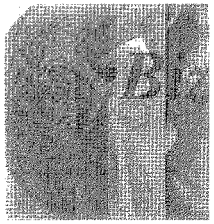
Authentication

Submission

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

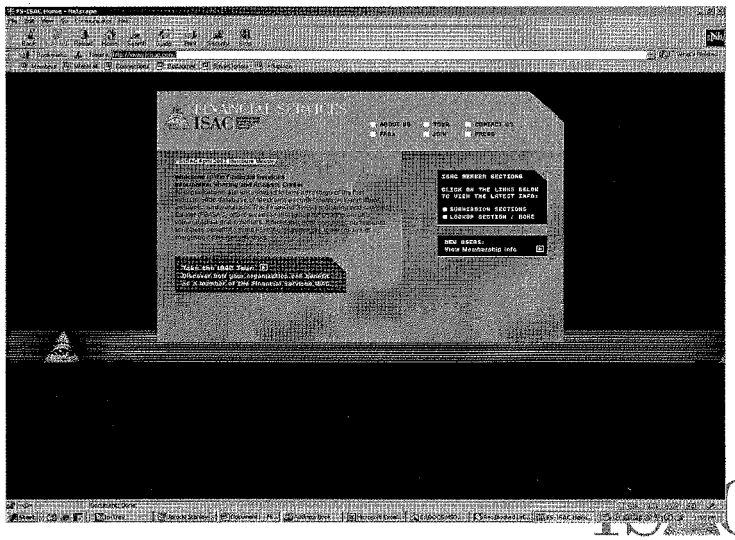
©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



FS/ISAC Website

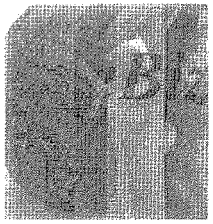
- **FS/ISAC Information**
  - *Overview*
  - *Membership*
  - *Tour*
  - *FAQs*
- **Submission**
  - *Anonymous*
  - *Attributable*
  - *Trusted*
- **Lookup**



INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



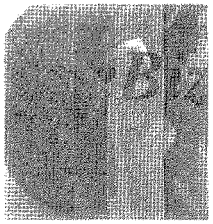
Membership Benefits

- *Early Notification* — Near-time notification gives maximum time to address incidents
- *Relevant Information* — Members receive focused data eliminating the need to sift through unnecessary detail
- *Industry-wide Vigilance* — Information sharing means each participant benefits from the combined experience of all members
- *Subject Matter Expertise* — Expert analysts ensure members are receiving the most accurate information possible
- *Anonymous Information Sharing* — Trusted information submissions without revealing one's identity facilitates cooperation while protecting proprietary interests
- *Trending* — Members early are provided with trend data on threats, vulnerabilities, and incidents impacting the financial services industry

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



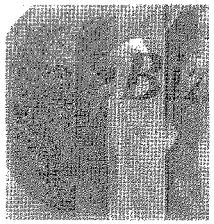
Membership

- **Membership pricing is designed to allow all eligible financial services companies to participate**
- **Membership levels:**
  - **Basic** — **Annual Fee: $7,000**
    (5 Attributable, 5 Anonymous Credentials, 2 Access Coordinators)
  - **Additional Users** — **Annual Fee: $100 / user**

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



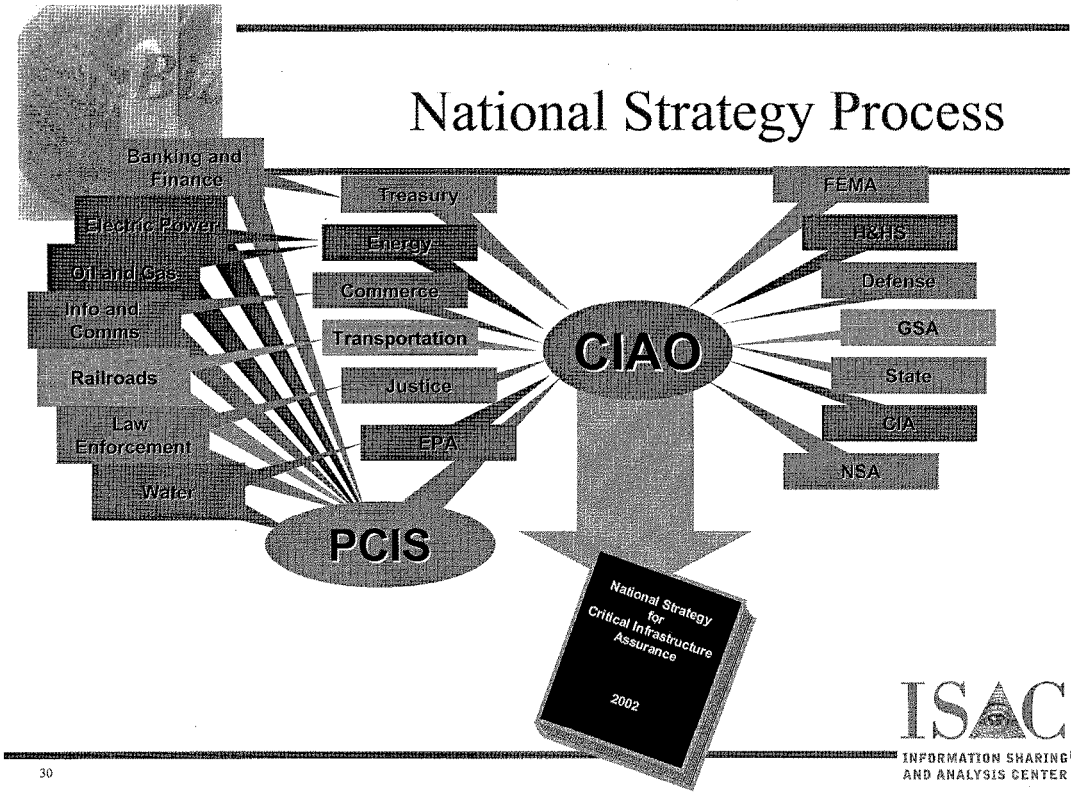
National Strategy

The Challenge for the New Frontier

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

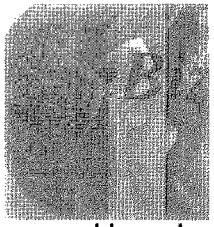
©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

National Strategy Process



ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



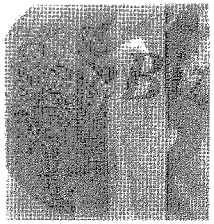
What needs addressing?

- How does each infrastructure sector view the risks and threats to service operations within its sector?
- How is the sector managing the risks posed by these threats?
- How does or should each company within the sector manage the risks posed by increased interdependencies?
- What does each sector see as the appropriate role of government and industry in dealing with these issues?
- Where does partnering make most sense for this infrastructure industry?
- What does the sector need from the government to proceed further in securing their operations? Specifically, what statutory, regulatory, or public policy reforms are needed?

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

2002 FS-ISAC LLC Proprietary, All Rights Reserved



Next Steps

- Establish a Roadmap to Success
- Formalize an Action Plan
- Obtain funding for actionable items
- Channel our energies
- To Vet or Not to Vet
  - Get Sector buy in
  - Understand the broad issues and concerns
  - Present unified positions to the Public

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©

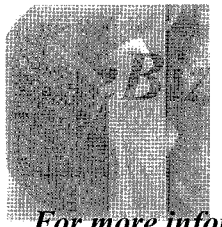
2002 VS-ISAC LLC Proprietary, All Rights Reserved

Vetting Processing

- 7/01 Position meeting
  - Treasury issues call to provide feedback to the Plan
  - BITS and FS/ISAC memberships redraft strategy based on new industry sector input
- August '01 – Treasury sponsored Sector meeting
- September '01 – Treasury issues National Plan II
- December '01 – Sector issues National Strategy for Critical Infrastructure Assurance V1 – draft to industry
- March 2002 – Banking and Finance Sector Vets National Strategy

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved



Contact Information

For more information on FS/ISAC:

Phone: (888) 660-0134;

Web Site: http://www.fsisac.com

Or Contact:

Stash Jarocki, Chairman
Phone: 718.754.2165; email: stash.jarocki@morganstanley.com

Suzanne Gorman, – Treasurer

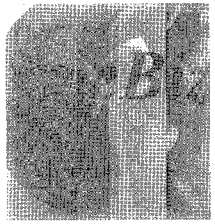
Phone: 212.383.9375 email: sgorman@siac.com

Fran Coppola, Coordinator
Phone: 212.855.8404; email: fcoppola@dtcc.com

Margie Sutphin, Coordinator
Phone: 703.480.3514; email: margie.sutphin@predictive.com

ISAC
INFORMATION SHARING AND ANALYSIS CENTER

© 2002 FS-ISAC LLC Proprietary, All Rights Reserved



?????

ISAC
INFORMATION SHARING
AND ANALYSIS CENTER

©
2002 FS-ISAC LLC Proprietary, All Rights Reserved

Statement of
David L. Sobel
General Counsel
Electronic Privacy Information Center

Before the
Senate Committee on Governmental Affairs

Hearing on
"Securing Our Infrastructure: Private/Public Information Sharing"

May 8, 2002
Washington, DC

Mr. Chairman and Members of the Committee:

Thank you for providing me with the opportunity to appear before the Committee to address the role that information sharing plays in the protection of our nation's infrastructure. The Electronic Privacy Information Center (EPIC) has a longstanding interest in computer and network security policy, emphasizing full and informed public debate on matters that we all recognize are of critical importance in today's inter-connected world.

While my comments will focus primarily on proposals to create a new Freedom of Information Act (FOIA) exemption for information concerning critical infrastructure protection, I would like to share with the Committee some general observations that I have made as this debate has unfolded over the past few years.

- There appears to be a consensus that the government is not obtaining enough information from the private sector on "cyber security" risks and vulnerabilities that could adversely affect the critical infrastructure. I hasten to add that citizens – the ones who will suffer the direct consequences of infrastructure failures – are also receiving inadequate information on these vulnerabilities.

- There has not yet been a clear vision articulated defining the government's proper role in securing the critical infrastructure. While there has been a great deal of emphasis on finding ways to facilitate the government's receipt of information, it remains unclear just what the government will do with the information it receives. In fact, many in the private sector advocate an approach that would render the government powerless to correct even the most egregious security flaws.

- The private sector's lack of progress on security issues appears to be due to a lack of effective incentives to correct existing problems. Congress

should consider appropriate incentives to spur action, but secrecy and immunity, which form the basis for many of the proposals put forward to date, remove two of the most powerful incentives – openness and liability. Indeed, many security experts believe that disclosure and potential liability are essential components of any effort to encourage remedial action.[1]

• Rather than seeking ways to hide information, Congress should consider approaches that would make as much information as possible available to the public, consistent with the legitimate interests of the private sector.

As indicated, I would like to focus my comments on proposals to limit public access to information concerning critical infrastructure protection. EPIC is a strong advocate of open government, and has made frequent use of the FOIA to obtain information from the government about a wide range of policy issues, including (in addition to computer security) consumer privacy, electronic surveillance, encryption controls and Internet content regulation. We firmly believe that public disclosure of this information improves government oversight and accountability. It also helps ensure that the public is fully informed about the activities of government.

I have personally been involved with FOIA issues for more than twenty years and have handled information requests on behalf of a wide range of requesters. In 1982, I assisted in the preparation of a publication titled *Former Secrets*, which documented 500 instances in which information released under the FOIA served the public interest. I am convinced that an updated version of that publication would today yield thousands of examples of the benefits we all derive from the public access law that has served as a model for other nations around the world.

EPIC and other members of the FOIA requester community have, for the past several years, voiced concerns about various proposals to create a broad new FOIA exemption, such as the one contained in S. 1456, for information relating to security flaws and other vulnerabilities in our critical infrastructures. We collectively believe this exemption approach is fundamentally inconsistent with the basic premise of the FOIA, which, as the Supreme Court has recognized, is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[2] To accomplish that end, "[d]isclosure, not secrecy, is the dominant objective of the Act."[3]

---

[1] *See, e.g.*, "Counterpane CTO Says Insurance, Liability to Drive Security," InfoWorld (February 20, 2002), <http://www.inforld.com/articles/hn/xml/02/02/20/020220hncounterpane.xml> (According to security expert Bruce Schneier, "[t]he challenges and problems of computer and network security won't be adequately addressed until companies can be held liable for their software and the use of their computer systems").

[2] *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

[3] *Department of the Air Force v. Rose*, 425 U.S. 352 (1976).

It is clear that, as we enter a new century and move further into the electronic age, the federal government increasingly will focus on the protection of critical infrastructures. It is equally apparent that government policy in this emerging field will become a matter of increased public interest and debate. EPIC has monitored developments in this area since the creation of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1997. After the Commission issued its report, EPIC published an analysis of the PCCIP's proposals (*Critical Infrastructure Protection and the Endangerment of Civil Liberties*[4]) which identified a number of Commission recommendations that could threaten privacy, extend the reach of federal law enforcement agencies, limit mechanisms for government accountability and increase the level of information classification and secrecy. While reasonable observers can disagree over the merits of such initiatives, I believe we all agree that critical infrastructure protection raises significant public policy issues that deserve full and informed public discussion.

Increasingly, government activity in this area will be conducted in cooperation with the private sector and, accordingly, will involve extensive sharing of information between the private sector and government. To facilitate the exchange of information, some have advocated enactment of an automatic, wholesale exemption from the FOIA for any "cyber security statements" or other similar information provided by a private party to a federal agency. Given the breadth of the proposed definitions of the categories of information to be exempted, I believe such an exemption would likely hide from the public essential information about critically important – and potentially controversial – government activities undertaken in partnership with the private sector. It could also adversely impact the public's right to know about unsafe practices engaged in by the private operators of nuclear power plants, water systems, chemical plants, oil refineries, and other facilities that can pose risks to public health and safety. In short, critical infrastructure protection is an issue of concern not just for the government and industry, but also for the public – particularly the local communities in which these facilities are located.

If the history of the FOIA is any guide, a new exemption would likely result in years of litigation as the courts are called upon to interpret its scope. The potential for protracted litigation brings me to what I believe is the most critical point for the Committee to consider, which is the need for the proposed critical infrastructure exemption. FOIA caselaw developed over the past quarter-century makes it clear that existing exemptions contained in the Act provide adequate protection against harmful disclosures of the type of information we are discussing. For example, information concerning the software vulnerabilities of classified computer systems used by the government and by defense contractors is already exempt under FOIA Exemption 1. Most significantly, Exemption 4, which protects against disclosures of trade secrets and confidential information, also provides extensive protection from harmful disclosures. Because I believe that Exemption 4 extends to virtually all of the material that properly could be withheld from disclosure, I would like to discuss briefly the caselaw that has developed in that area.

---

[4] http://www.epic.org/security/infowar/epic-cip.html

For information to come within the scope of Exemption 4, it must be shown that the information is (A) a trade secret, or (B) information which is (1) commercial or financial, (2) obtained from a person, and (3) privileged or confidential.[5] The latter category of information (commercial information that is privileged or confidential) is directly relevant to the issue before the Committee. Commercial or financial information is deemed to be confidential "if disclosure of the information is likely to have either of the following effects: (1) to impair the government's ability to obtain the necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained."[6] The new FOIA exemption that has been proposed seeks to ensure that the government is able to obtain critical infrastructure information from the private sector on a voluntary basis, a concern which comes within the purview of Exemption 4's "impairment" prong. The courts have liberally construed "impairment," finding that where information is voluntarily submitted to a government agency, it is exempt from disclosure if the submitter can show that it does not customarily release the information to the public.[7] In essence, the courts defer to the wishes of the private sector submitter and protect the confidentiality of information that the submitter does not itself make public.

In addition to the protections for private sector submitters contained in FOIA Exemption 4 and the relevant caselaw, agency regulations seek to ensure that protected data is not improperly disclosed. Under the provisions of Executive Order 12600 (*Predisclosure Notification Procedures for Confidential Commercial Information*) issued by President Reagan in 1987, each federal agency is required to establish procedures to notify submitters of records "that arguably contain material exempt from release under Exemption 4" when the material is requested under the FOIA and the agency determines that disclosure might be required. The submitter is then provided an opportunity to submit objections to the proposed release. The protections available to private sector submitters do not end there; if the agency determines to release data over the objections of the submitter, the courts will entertain a "reverse FOIA" suit to consider the confidentiality rights of the submitter.[8]

In light of the substantial protections against harmful disclosure provided by FOIA Exemption 4 and the caselaw interpreting it, I believe that any claimed private sector reticence to share important data with the government grows out of, at best, a misperception of current law. The existing protections for confidential private sector information have been cited repeatedly over the past two years by those of us who believe that a new FOIA exemption is unwarranted. In response, exemption proponents have not come forward with any response other than the claim that the FOIA creates a

---

[5] *Getman v. NLRB*, 450 F.2d 670, 673 (D.C. Cir. 1971), *stay denied*, 404 U.S. 1204 (1971).

[6] *National Parks and Conservation Association v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974).

[7] *Critical Mass Energy Project v. Nuclear Regulatory Commission*, 975 F.2d 871 (D.C. Cir. 1992) (*en banc*), *cert. denied*, 113 S.Ct. 1579 (1993).

[8] *See GTE Sylvania, Inc. v. Consumers Union*, 445 U.S. 375 (1980).

"perceived" barrier to information sharing.[9] They have not provided a single example of voluntarily submitted information that would not fall within the protection of Exemption 4.

Frankly, many in the FOIA requester community believe that Exemption 4, as judicially construed, shields far too much important data from public disclosure. As such, it is troubling to hear some in the private sector argue for an even greater degree of secrecy for information concerning vulnerabilities in the critical infrastructure. As I have noted, shrouding this information in absolute secrecy will remove a powerful incentive for remedial action and might actually exacerbate security problems. A blanket exemption for information revealing the existence of potentially dangerous vulnerabilities will protect the negligent as well as the diligent. It is difficult to see how such an approach advances our common goal of ensuring a robust and secure infrastructure.

In summary, the Freedom of Information Act has worked extremely well over the last 25 years, ensuring public access to important information while protecting against specific harms that could result from certain disclosures. After monitoring the development of critical infrastructure protection policy for the last several years, I have heard no scenario put forth that would result in the detrimental disclosure of information under the current provisions of the FOIA. Overly broad new exemptions could, however, adversely impact the public's right to oversee important and far-reaching governmental functions and remove incentives for remedial private sector action. I urge the Committee and the Congress to preserve the public's fundamental right to know.

David L. Sobel is General Counsel of the Electronic Privacy Information Center in Washington, DC, a non-profit research organization that examines the privacy implications of computer networks, the Internet and other communications media. He has litigated numerous cases under the Freedom of Information Act (FOIA) seeking the disclosure of government documents on privacy policy, including electronic surveillance and encryption controls. Among his recent cases are those involving the Digital Signature Standard, the Clipper Chip and the FBI's Carnivore Internet surveillance system. Mr. Sobel also served as co-counsel in *ACLU v. Reno*, the successful constitutional challenge to the Communications Decency Act decided by the U.S. Supreme Court in 1997.

Mr. Sobel has a longstanding interest in civil liberties and information access issues and has written and lectured on these issues frequently since 1981. He was formerly counsel

[9] *See, e.g.*, Letter from Daniel P. Burnham, Chair, National Security Telecommunications Advisory Committee to the President, June 28, 2001 ("*Real or perceived*, barriers to [information] sharing must be removed. Among those barriers are the Freedom of Information Act and potential legal liabilities") (emphasis added).

to the National Security Archive, and his FOIA clients have included Coretta Scott King, former Ambassador Kenneth Rush, the Nation magazine and ABC News.

Mr. Sobel is a graduate of the University of Michigan and the University of Florida College of Law. He is a member of the Bars of Florida, the District of Columbia, the U.S. Supreme Court and several federal Courts of Appeals.

Disclosure

Neither Mr. Sobel nor the Electronic Privacy Information Center has received any federal grants and/or contracts during the current fiscal year or either of the two previous fiscal years.

Testimony

Submitted by

Rena Steinzor

on behalf of the

Natural Resources Defense Council

Mr. Chairman and members of the Committee, thank you for the opportunity to appear before you today to testify regarding the management of critical infrastructure information on behalf of the Natural Resources Defense Council (NRDC). NRDC is a national, non-profit organization of scientists, lawyers, economists, and other environmental specialists dedicated to protecting public health and the environment. Founded in 1970, NRDC has more than 500,000 members nationwide, and four national offices in New York, Washington, Los Angeles, and San Francisco.

The issues before you are both significant and troubling, especially in the wake of the tragedies that began on September 11, 2001. Obviously, all Americans recognize the importance of doing whatever we can to improve homeland security. At the same time, this country was attacked because we are the most successful democracy the world has ever known. If we overreact to those who attacked us so viciously, and in the process undermine the principles and rule of law that have made us such a hopeful example for the world, terrorists will win the victory that has thusfar eluded them.

In the testimony that follows, I explain NRDC's strong opposition to both the text and the underlying principles embodied in S. 1456, the "Critical Infrastructure Information Act," and our proposals regarding how the problems that underlie the legislation should be handled. Before I launch into that analysis of the legislation's flaws, however, I want to thank Senators Bennett and Kyl for their commitment to work with public interest groups to address these problems. We have received informal assurances that several of our problems will be addressed in subsequent drafts of the legislation. Nevertheless, because no alternative language has yet become available and because certain industry supporters of the legislation have reiterated support for the original language as recently as a few weeks ago, we are compelled to remain forceful, as well as vigilant, in urging you to oppose it.

My testimony addresses the following four central points:

1. ***The legislation has an impossibly broad scope.***
2. ***The legislation will have a series of disastrous, unintended consequences, damaging existing statutory frameworks crafted with care over several decades.***
3. ***Secrecy is not the best way to protect critical infrastructure, and this Committee should abandon that approach. Rather, Congress should require covered industries to conduct assessments of their vulnerabilities and take effective action to eliminate terrorist targets.***
4. ***As the Committee continues its consideration of the legislation, it is vital that a broad range of experts and stakeholders participate in those deliberations.***

I have attached a detailed analysis of S. 1456 to my testimony and ask that it be made part of the record of this hearing.

Scope

In a sense, S. 1456 is a piece of legislation with multiple personalities, perhaps because it has several, at times inconsistent, goals.

As I understand it, the bill was drafted before September 11, and is an outgrowth of the successful management of the "Y2K" crisis. That is, the central purpose of the bill is to facilitate the collaboration between industry and government that produced the effective response to what could have been a devastating failure of computer systems here and around the world.

To the extent that the legislation focuses on "cyber systems" – and by these I mean systems that are connected to the Internet and therefore are vulnerable to outside disruption -- NRDC as an institution has little to add to the debate. Computers are not our area of expertise. Indeed, some of our computers have not made it past Windows '95 operating systems.

As a consumer of computer products, I must confess that I wonder how companies will

be held accountable for doing everything feasible to prevent cyber-attacks if they are allowed to keep the details of how they responded to notices of such problems secret and are immunized from liability to their customers. But I leave a detailed exploration of the best approaches to these purely cyber problems to other members of this panel.

Of course, S. 1456 extends much further than cyber systems, covering not just computers that are connected to the Internet, but also the physical infrastructure used to house these systems. The legislation covers not just any physical infrastructure that is connected to, and therefore would be affected by a cyber attack through the Internet, but also any physical infrastructure that is "essential" to the "economy" and that might be damaged by a physical attack. Its coverage is so breathtakingly broad that at some point one begins to suspect that simple collaboration to prevent cyber interference may have been where it all started, but that along the way its goals became far more complex and ambitious.

NRDC is sensitive to the fears all Americans have about our vulnerability to terrorist attacks. We are active participants in the debates that continue in other contexts about whether information about the operations of facilities storing acutely toxic chemicals should be accessible on the Internet or in other contexts. On one hand, we understand the need to keep information out of the hands of potential attackers. On the other hand, we believe that the communities that would be directly affected by such catastrophes need access to information necessary to assess and respond to these threats, both before and after they materialize. Suffice it to say that the Environmental Protection Agency (EPA) is encountering many challenges as it works diligently to sort through these issues and made decisions whether to revise our approach to information about chemical use in the "post 9/11" world.

However, with all due respect to this Committee, these difficult issues are not within the areas of expertise of the government agencies assigned a role in implementing S. 1456. Further, this Committee has not focused its resources on examining these questions historically. To the extent that S. 1456 has become a vehicle for addressing how disclosure of information plays a role in enhancing or combating the terrorist threat to physical infrastructure, you have a daunting

and arguably duplicative task before you.

Consequently, NRDC urges you to eliminate from consideration the security of information pertaining to any aspect of physical infrastructure, even facilities that are connected in some way to cyber systems.

Unintended Consequences

Several years ago, major industry trade associations with members subject to environmental regulations began to push the idea of giving companies immunity from liability if they performed "self-audits," uncovered violations of the law, took steps to solve those problems, and turned the self-audit over to the government voluntarily. The Department of Justice vigorously opposed such proposals, and they never made it through the Congress. Several states enacted versions of self-audit laws. In the most extreme cases, EPA responded by threatening to withdraw their authority to implement environmental programs and the laws were repealed.

The reasons cited by the Justice Department and EPA are instructive. Our system of law is based on "deterrence-based" enforcement. Or, in plain English, the prospect of getting caught is sufficiently probable and the consequences sufficiently distasteful that large numbers of regulated entities are reminded of those incentives to comply every time the government brings an enforcement action against one of their number. The government cannot prosecute all violators, and no one expects it to do so. But enforcement is frequent enough to shorten the odds and make compliance the rule, not the exception.

Self-audit bills defeat this dynamic, creating a situation where amnesty is available even where a company has cynically continued in violation for many years, "discovers" its behavior, and does nothing more than come into compliance at the last minute. The large costs avoided by such scofflaw behavior are never recovered and the company, not the government, is in charge of what can only loosely be characterized as an enforcement process.

As drafted, S. 1456 is a breathtakingly comprehensive self-audit bill that extends not just

to environmental violations, but to violations of the nation's tax, civil rights, health and safety, truth-in-lending, fraud, environmental, and virtually every other civil statute with the exception of the Securities Act. (For reasons that have never been explained, the legislation explicitly exempts the Securities Act from its secrecy provisions, setting up an anomaly where wealthy investors will still have access to the courts while all other injured consumers and customers are shut out.) The legislation does not even require that companies cure their violations in order to receive amnesty. Rather, it allows them to simply stamp materials as secret "critical infrastructure information" and turn them over to the officials designated by the Office of Management and Budget, which would have the responsibility of ensuring that the information is never used against the submitter in a civil action in court.

Staff for Senators Bennett and Kyl have explained that these consequences were not intended when they wrote the legislation, and NRDC therefore awaits a new draft of the bill before making a final judgment. But we cannot let this moment pass without expressing our profound doubts that a redraft can solve the problem easily. As long as industry is allowed to assert that information must remain secret without making any showing as to why, and no government officials are assigned to scrutinize and validate such claims upfront, it will be a nightmare to straighten the situation out after the fact, especially if "critical infrastructure information" continues to have such a broad definition.

To illustrate the problem, imagine that a company discovers that it has a tank of acutely toxic chemicals that is old and prone to leaks. The instrument panel for the tank is accessible to even its most casual employees and other visitors to the plant site, but it does not wish to bear the costs of moving the panel or replacing the tank. Someone in the general counsel's office gets the bright idea of taking pictures of this "vulnerable" infrastructure, writing a detailed report, and sending them over to the Homeland Security Office, where they join hundreds of thousands of other documents warehoused throughout the Washington area. Later, an EPA or OSHA safety inspector arrives, notices this dangerous situation, and tries to assess civil penalties against the company. The subsequent litigation turns not on whether the conduct was a violation of the law,

but rather on whether the information is indeed critical infrastructure information. Most importantly, the problem is never fixed and the company is protected from the consequences of its grossly negligent activities.

Does anyone think for even a moment that it is worth setting up such miserable legal stalemate on the off chance that disclosure of this information months or years later, pursuant to a Freedom of Information Act request or civil discovery, might increase the vulnerability of the tank to a terrorist attack? Surely there is a better way.

The next section of my testimony explains how a sister Committee and EPA are working to find a better way, but before I leave the area of unintended consequences, I would like to offer for the record a document I prepared explaining what questions must be considered if the sponsors are intent on redrafting their bill. We are far from convinced that even the best drafters could avoid serious unintended consequences, but if the sponsors are intent on pursuing this course of action, we implore you to use these questions to determine how close you are coming to that mark.

Secrecy Is Not the Answer

In the eight months since September 11, thousands of people have spent many hours working on policies and requirements that will strengthen homeland security. The scenario I just presented involving the tank storing acutely toxic chemicals is a good vehicle to illustrate the content of those efforts.

One way to reduce the vulnerability of the tank to a terrorist attack is to ensure that only employees who have undergone background checks and are rigorously supervised are allowed in the vicinity of the tank. This approach involves both site security at the fence-line of the facility and in the area adjacent to the tank, as well as greater vigilance in selecting workers. Another way to make the tank more secure would be to move it, the instrument panel that operates it, and – for that matter – the computer system that connect them inside a locked fence or other barrier. But by far the most effective way to protect the public and the workers from the devastating

effects of an equipment failure at a facility capable of releasing gases that kill on contact is to eliminate the need for the chemical and therefore the tank itself.

This approach is called "inherently safer technology" and involves ensuring that everything that can be done is done to eliminate or reduce the storage of acutely toxic chemicals at the site. Inherently safer technology is the cornerstone of legislation introduced by Senators Corzine, Jeffords, Clinton and Boxer now under consideration by the Senate Environment and Public Works Committee. S. 1602, the "Chemical Security Act of 2001," would require EPA to regulate the efforts companies make to enhance site security and eliminate potential targets, efforts that actually solve the problem rather than sweeping it out of public view. Senator Corzine is now in the process of refining the bill to ensure that companies have the flexibility they need to assess the vulnerability of physical infrastructure and take the most effective action to prevent terrorist attacks.

NRDC has also consulted with EPA officials responsible for coordinating their Agency's contribution to strengthened homeland security. EPA has extensive legal authority to take action against companies that fail to exercise due diligence in preventing such attacks, and we are heartened to see that staff appear to be making a comprehensive effort to develop a plan for using that authority most effectively. Hopefully, the combination of the Corzine bill and administrative action will make great strides in the foreseeable future toward addressing the problems I have described above.

NRDC believes that actually requiring changes, on-the-ground, as required by S. 1602 and EPA's existing legal authority, is a far preferable solution to the threats we face than giving companies and the government an opportunity to sweep such problems under the rug. Further, although cyber systems are not within our area of expertise, we are certain that pursuit of new technologies to forestall or blunt cyber attacks by terrorist or other criminal actors is a far more productive use of the nation's limited resources than bickering endlessly, in and out of court about what information can, should, or would be protected from disclosure.

Process

In the last few weeks, Committee staff, under the direction of Senators Lieberman and Thompson, have undertaken a series of discussions with groups potentially affected by S. 1456 to better understand the policy goals and implications of the legislation. NRDC was included in these discussions, and we appreciate the diligence with which they have been pursued. We hope that this hearing marks the continuation of that kind of collaboration, rather than its end point. For all the reasons stated above: the pressing need to strengthen homeland security, the potential unintended consequences of the legislation as currently drafted, and the availability of far more effective alternatives, we believe that stakeholders with varied expertise must continue to participate in this unfolding legislative process. If NRDC had its druthers, the approach taken in S. 1456 would be dropped in favor of more direct action to solve the problem. Whether or not we get our wish, however, our perspective is an important part of this debate, as are the perspectives of those who disagree with us.

Thank you, Mr. Chairman and members of the Committee. I would be pleased to answer any questions you may have.

November 25, 2001

Problems with S. 1456
Critical Infrastructure Information Act

*Note: **Problems are listed in the order in which they appear in the draft of the legislation dated November 6, 2001, and not necessarily in the order of their importance.***

Sec. ___ 02. FINDINGS.

FINDING (8): Page 4, lines 15-25 and page 5, lines 1-5:

These paragraphs indicate congressional intent to apply the legislation as broadly as possible to virtually every sector of the economy. They further state that in order to encourage voluntary submission of any information about any aspect of an industry's physical infrastructure, the government must pledge not to disclose it if disclosure would "result in legal liability or financial harm."

The scope of this language goes far beyond efforts to preserve the security of computer systems or even physical plants in the event of a criminal attack. Rather, the language clearly invites all sectors of the economy to submit any information they would prefer to keep confidential ***in order to avoid legal liability or financial harm.*** Thus, for example, companies could submit information about illegal acts they have committed, from tortious conduct to tax fraud, and be protected from having the information used to hold them accountable.

FINDING (9): Page 5, lines 6-13:

This provision compounds the impression that the legislation could be used as a source of amnesty for legal violations by specifically encouraging companies to engage in "risk assessments" and "risk audits," turn such information over to the government, and thereby preclude its use in any subsequent prosecution of the company. In the environmental arena, "risk audit" is a term of art meaning an evaluation of a company's compliance with the nation's environmental laws. For many years, industry has engaged in an ***unsuccessful*** effort to persuade Congress to grant exactly this type of self-audit privilege. Congressional committees have rejected these proposals because they would encourage chronic violators to periodically purge themselves of the consequences of their violations by turning the results of their internal audits over to the government.

FINDING (13): Page 6, lines 13-17:

This finding – stating that the information covered by the bill is "not normally in the public domain" -- is clearly erroneous, suggesting that the legislation has a far broader scope than its authors may have intended. A large majority of the information regarding normal industrial operations that would be protected from disclosure if the legislation is enacted into law is routinely in the public domain, and has been for several decades.

Sec. ___04. DEFINITIONS.

Section 04 (4) "Critical Infrastructure": Page 9, lines 3-25, page 10, lines 1-2:

Paragraph (4)(A) applies the legislation's non-disclosure provisions to virtually any aspect of a company's normal operations by including "physical, information, and data systems and services essential to . . . [the] economy of the United States." The legislation does not require that the impact on the economy be significant or that the damage have some effect on the national security. Under this definition, the smallest, temporary malfunction of any piece of equipment would be covered, even if it caused no lasting damage to a company's performance. Major damage caused by the company's own negligence would be similarly protected.

The definition further encompasses "all types of communications and data transmission systems, electric power, gas and oil production, refining, storage, transportation and distribution, banking and finance, transportation [sic] water supply, emergency services . . . the continuity of government operations, and their associated protected or essential systems." Under this broad language, routine monitoring of emissions of toxic chemicals into the air, discharges of toxic chemicals into water, or the level of toxic chemicals in the ambient air within a workplace could be kept secret if the company claimed that disclosure would "affect" the economy. This extraordinarily broad coverage is far more extensive than critical computer system information necessary to launch a terrorist attack.

Completing the effort to draw as wide a parameter as possible for the scope of the legislation, paragraph 04(b) includes "any industry sector designated by the President pursuant to the National Security Act of 1947 . . . or the Defense Production Act of 1950." These statutes give the President the authority to designate any industry that now sells – or might sell – products to the United States military, encompassing everything from armaments to baseball caps and suntan lotion.

Section 04 (5) "Critical Infrastructure Information": Page 10, lines 3-25, page 11, lines 1-2:

This definition continues to define an extremely broad scope for the legislation. The first subparagraph – (5)(A) – covers the information that is the ostensible focus of the bill, namely the ability of critical infrastructure to resist criminal interference. Even in this relatively discrete provision, however, the temptation to extend the legislation's parameters surfaces when it covers "attack[s] or similar conduct" that "harms interstate commerce," whether or not the conduct was criminal. Since "harm" to interstate commerce can include even minor damage, this provision encompasses non-criminal, even inadvertent conduct that causes any temporary interruption of normal business operations.

The next three subparagraphs – (5)(B), (C), and (D) – are even broader in application, extending the legislation's secrecy provisions to "any planned or past assessment . . . of the security vulnerability of critical infrastructure . . . including . . . risk management planning, or risk audit." Since "security" is not defined in the legislation, but commonly means the safety of

a system or set of industrial practices, this provision encompasses any analysis of a company's vulnerability not just to an attack, but to normal malfunctioning of equipment, human operational errors, or system failure. As noted earlier, the manufacturing sector has attempted unsuccessfully for years to persuade Congress to grant ***immunity from civil liability for violations of health and safety regulations, including those issued by EPA or OSHA***, if it conducts risk audits and submits them to the government. This provision would have the same effect as that rejected legislation, circumventing the normal legislative process and bypassing the committees that have considered these proposals and rejected them in the past.

Finally, subparagraph (5)(C) of the legislation protects the confidentiality of information about "any planned or past operational problem or solution, including repair, recovery, reconstruction . . . related to the security of critical infrastructure." This provision, while in certain respects redundant with subparagraph (5)(B), confirms legislative intent to cover the expansion of a facility's operating equipment in order to address past problems, effectively shrouding the unpermitted construction of new sources from EPA review. Thus, a company could replace the equipment of a "major source" as defined by the Clean Air Act, producing a new operating system that discharges twice the emissions, without applying to EPA for a new permit, and EPA could do nothing to enforce the law if information about construction of the new source was submitted "voluntarily" to the government.

Section 04 (6) "Information Sharing and Analysis Organization": Page 11, lines 3-25, page 12, lines 1-2:

This provision invites the creation of industry trade associations called "information sharing and analysis organizations" (ISAO), for the explicit purpose of gathering and submitting information that would be covered by the confidentiality protections of the legislation. *(See also subparagraph (8)(A), page 12, lines 17-25 and page 13, lines 1-2, explicitly inviting ISAOs to submit information "voluntarily" on behalf of their members.)* Since freedom from civil enforcement would be a tremendous advantage to potential members of such organizations, it is likely that every major corporation will be solicited for membership in an ISAO, and will take full advantage of the bill's protections. Smaller competitors of such large entities may not be solicited, or may conclude that they cannot afford the dues or other fees charged by ISAO, making them targets for frustrated government enforcement programs, an outcome contrary to sound public policy and basic fairness.

Section 04 (7) "Protected System": Page 12, lines 3-16:

This definition confirms the broad application of the legislation's secrecy provisions to "any service, physical or computer-based system, process or procedure that directly or indirectly affects a facility of critical infrastructure." Under this overreaching language, the malfunctioning of a stove in the corporate cafeteria could fall within the legislation's scope, an absurd but obvious result of such expansive language.

Section 04 (8) "Voluntary": Page 12, lines 17-25, page 13, lines 1-23, page 14, lines 1-2:

This crucial provision defines "voluntary" submission to include any conveyance of covered information by a covered entity with respect to a covered facility and a covered threat. The only limitation on this broad scope is that the submittal of the information must be made "in the absence of such agency's exercise of legal authority to compel access to or submission of such information." While this language is admittedly ambiguous, it could be read to include any information submitted by a company that is not already the subject of a subpoena or other access order compelling disclosure of the information. Because the provision uses the present tense, requiring that the agency ***has exercised*** its legal authority, the exclusion it creates is significantly narrower than an exclusion tied to coverage of the information by another legal authority that could be exercised at some time by an agency. Therefore, the definition of "voluntary" explicitly encourages companies to rush to submit information under the legislation in order to avoid some subsequent exercise of subpoena or other legal authority by a regulatory agency. Once covered by the legislation's secrecy provisions, the information could not be disclosed by the agency, to anyone – including a civil court judge – in perpetuity. *(For the text of these sweeping protections, see Section 05, pages 14, lines 4-25, page 15, lines 1-25, page 16, lines 1-25, page 17, lines 1-25, page 18, lines 1-4.)*

The legislation underscores and confirms this excessively broad definition of a "voluntary" submission by specifically excluding from the exclusion information involved in any ***ongoing action*** brought under the Securities Exchange Act. Or, in plain English, even if the SEC has not subpoenaed such information in an action it has already filed, the company is precluded from taking advantage of the legislation's confidentiality provisions and the information can be used to prosecute the civil case. Under standard principles of statutory interpretation, this exclusion will be read to mean that if the IRS, the Departments of Justice or Defense, EPA, OSHA, or any other agency or department is prosecuting a civil action for tax evasion, contractor fraud, violations of environmental permits or workplace safety standards, the company can preclude use of information that was previously submitted "voluntarily" whether or not it receives a government subpoena.

The legislation further excludes from the exclusion "information or statements required as a basis for making licensing or permitting determinations." Or, in other words, information that agencies or departments specifically direct applicants to include in their requests for permits or licenses can be disclosed. Any information submitted voluntarily as part of a permit application, or submitted later to demonstrate compliance with the permit, presumably would be kept confidential.

Sec. ___ 05. PROTECTION OF VOLUNTARY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

Section 05(a) "Protection": Page 14, lines 4-25, page 15, lines 1-25, page 16, lines 1-3:

This section explicitly repeals all other provisions of law, including state and local laws, that pertain to the information and entities covered by the legislation's provisions, as explained above because it opens with the unequivocal statement "[n]otwithstanding any other provision of law . . ." as an introduction to its confidentiality protections.

The section further provides that "critical infrastructure information . . . that is voluntarily submitted to a covered Federal agency . . . for [any] informational purpose . . . shall be exempt from disclosure" under the Freedom of Information Act. This broad prohibition means that federal agencies will be barred from disclosing unknown quantities of information that they routinely disclosed before to citizens, and to state and local appointed and elected officials, including local prosecutors, and police and firefighting personnel unless some other provision of law other than the Freedom of Information Act authorizes such disclosure.

Even if disclosure to state and local enforcement officials or emergency personnel is authorized by another law, the legislation bars disclosure if the federal agency has not received the "written consent" of the "person or entity" that submitted it. The information covered by this broad prohibition includes not only "critical infrastructure information" itself but also the "identity of the submitting person or entity." Disclosure is barred "in any civil action arising under Federal or State law if such information is submitted in good faith," thereby precluding any and all enforcement actions. Although the legislation does not repeal the enforcement powers of federal agencies and departments, no target of an investigation would voluntarily settle its case if the federal agency or department was legally precluded from bringing the matter to court. The explicit identification of civil actions leaves no doubt that the intent of the legislation is to provide immunity from civil violations.

The legislation would also accomplish an unprecedented preemption of state liability laws, including the common law of tort allowing victims of chemical exposure to recover damages, because it states that "critical infrastructure information . . . shall not, without the written consent of the person or entity submitting such information, be used by any third party in any civil action." This provision could be read to mean that if "critical" information is first submitted to a federal agency, a company need not disclose in any subsequent litigation brought by any private citizen. The sponsors may have intended merely to preclude a private third party from using the ***government's copy of the information*** in a civil action, allowing private parties to gain access to other copies of the information, including copies maintained by the company, through the normal judicial process. However, this limitation is nowhere specified in the legislation, which speaks generally of "critical information" without specifying any particular custodian or version.

Further compounding these problems, the federal agency or department is barred from using or disclosing the information, including the identity of the submitter, without the

submitter's written consent for any other purpose with only two exceptions. Unless disclosure is covered by one of these two exceptions, agencies and departments may not rely on voluntarily submitted information, including the identity of the submitter, when they are crafting regulatory provisions; issuing guidance regarding interpretations of the laws under their jurisdiction; conducting routine inspections of facilities selling food and other products to the public; responding to congressional requests for information; or performing studies and compiling reports not explicitly required by the legislation itself.

It is not an overstatement to suggest that this extraordinarily broad prohibition on disclosure could bring the normal regulatory process to a grinding halt, placing great pressure on those two exceptions.

The first exception permits disclosure during the "proper performance of the official duties of an officer or employee of the United States." *(See section 05(a)(D)(ii) on page 15, lines 8-10.)* The underlined terms have been interpreted by the courts extensively in the context of enforcement of section 1983 of the U.S. Code, which provides for punishment of federal and local officials who abuse civil rights. Such officials may not be held liable if they were performing their official duties properly, and the law has evolved in a manner that takes into account multiple nuances and implications of this ambiguous wording. In any given factual circumstance, extensive legal research and analysis would be necessary to find precedent indicating what those terms mean. If the legislation becomes law, it is entirely possible, even likely, that this exception will be interpreted narrowly and, since the legislation explicitly prohibits any legal challenge to its implementation, the courts will be barred from intervening to assist in the correct application of this language. *(See Section 08, page 26, lines 22-25, barring private rights of action to enforce the legislation's provisions.)*

In sum, the first exception does nothing to narrow the scope of the legislation unless the federal, state, and local officials implementing its provisions decide in their discretion to so limit it. Further, one official might assert that he is exercising his authority appropriately and wishes to disclose information, only to be contradicted by another official with a different motivation to keep the information secret.

The second exception is that information may be disclosed "in furtherance of an investigation or prosecution of a criminal act." *(See Section 05(a)(1)(D)(ii), page 15, lines 11-12.)* This exception is unambiguous and fortunate.

Section 05(b) "Independently Obtained Information": Page 16, lines 4-12

This crucial provision may have been intended as a "savings clause" to counteract the drastic implications of Section 05(a) discussed immediately above. Unfortunately, the language of the subsection is so garbled that it may well be read to have no effect on the legislation's broad prohibitions on disclosure. The language reads: "Nothing in this section shall be construed to limit or otherwise affect the ability of a state, local, or Federal government entity . . . to obtain critical infrastructure information in a manner not covered by subsection (a) . . . and to use such information appropriately." Read in the context of the other provisions of subsection 05 (a), including and especially the ban on disclosing information unless it was previously subpoenaed,

this provision is likely to be read to mean that any information that ***is*** covered by subsection (a) must be kept confidential. Thus, the savings clause would only cover information that is ***not*** covered by subsection (a): that is, information that was not "voluntarily" submitted to the government. In effect, this provision penalizes companies that are too ignorant to submit sensitive information voluntarily, but fails to preserve the essential government enforcement and rulemaking authorities nullified by subsection (a).

Section 05(c) "Treatment of Voluntary Submittal of Information": Page 16, lines 13-18:

This provision, potentially another "savings clause" for other provisions of federal law requiring companies to submit information to the government, also fails to circumscribe the legislation's secrecy provisions appropriately. The provision states that voluntary submittal of information to – for example – the White House Homeland Security Office or the Department of Defense – does not "constitute compliance" with other requirements that the covered entity submit the information to another agency or department. The provision does ***not*** say that if the information is submitted to another agency or department, that agency or department may disclose it even if confidentiality has been claimed in the submission to the Homeland Security Office or DOD. Thus, a plausible interpretation of this provision is that a company can submit the information voluntarily first, claiming that it is entitled to confidential treatment, and then resubmit it to a second agency or department, claiming the same right to confidential treatment. The second submission complies with the independent requirement that the information be submitted without jeopardizing the goals of the legislation. Indeed, to read the provision any other way would arguably vitiate the legislation's findings, purpose, and legal effect.

February 18, 2002

Questions to Clarify Intent of S. 1456

Prepared by Rena Steinzor, Natural Resources Defense Council
(202) 289-2364 or rsteinzor@nrdc.org

Note: Participants in the debate over the Critical Infrastructure Information Act (S. 1456) have strongly disagreed not only about the policy goals of the legislation, but also with respect to what its key provisions mean. Confusion over the intent of the language has obscured and frustrated the discussion and resolution of legitimate policy disputes. The following questions are an effort to clarify the intent of the language so that perceived drafting problems can be addressed, allowing the debate to focus on those core policy issues.

Threshold Assumptions:

What evidence exists to document whether and why companies refuse to share sensitive cyber security information with the government?

Why do companies fear that information submitted voluntarily, will be made public under the Freedom of Information Act, given the D.C. Circuit Court of Appeals holding in the Critical Mass case (975 F.2d 871 (1992)) that such materials are exempt from disclosure?

Circumstances Covered:

Is the legislation intended to cover:

a. attacks from one computer system to another ("cyber attacks") – e.g., hackers send Love Bug to U.S. computers supporting the Pentagon;
b. attacks from one computer system to another that result in damage to physical infrastructure (e.g., hackers send Love Bug to computers controlling the operation of the Power Grid, resulting in black-out that causes heavy machinery to break down); or
c. attacks on physical infrastructure that damage cyber systems (e.g., terrorist plant bomb in building that houses server for power supply company).

Consequences Covered:

Is the legislation intended to:

a. eliminate use of voluntarily submitted "critical infrastructure information" to support legal liability in civil law cases brought in a public law context (e.g., company X turns in documents labeled "critical infrastructure information" indicating that it has evaded tax laws by depreciating equipment too quickly);

b. eliminate use of critical infrastructure information to support civil liability in a private law context (company X turns in documents indicating that it is aware of weaknesses in a manufacturing process and these weaknesses result in an explosion that badly injures nearby residents, who sue to recover damages);
c. affect the federal government's ability to share information among agencies and departments (e.g., the information described in (a) is turned over to the Homeland Security Office and subsequently requested by the IRS); or
d. affect the federal government's ability to share information with state and local officials (e.g., the information described in (b) is requested by a state environmental agency investigating possible violations of the laws it administers).

Type of Information Covered:

The legislation defines "critical infrastructure information" as information "related to the "ability of any critical infrastructure" to "resist interference, compromise, or incapacitation by either physical or computer-based attack or other similar conduct. Is the legislation intended to cover:

a. computer security systems intended to prevent cyber attacks;
b. security systems intended to prevent physical attacks;
c. information regarding the operation of a manufacturing process that could be used to either choose the facility as a target or to promote a cyber or physical attack;
d. information about the company's products or customers that could be used to either chose a facility as a target or to promote a cyber or physical attack;
e. administrative or financial details regarding a company's operation that might suggest that its facilities would make good targets or that would promote a cyber or physical attack (e.g., the company has suspended required maintenance because it has encountered financial difficulties or the company's union contract with operating engineers is about to expire); or
f. vulnerability of any aspect of the company's operation to misconduct attacks by its own employees. For example, misconduct "similar to a cyber or physical attack" might include administrative fraud or omissions or a slow-down in work performance by disgruntled workers.

Status of Covered Information:

The legislation's findings state that it is intended to cover information that would not "normally [be] in the public domain," but this caveat is not repeated in the legally operative portions of the bill. Is the legislation intended to cover:

a. information that the law requires companies to keep but that they do not routinely turn over to the government;
b. information that the company elects to keep to demonstrate its compliance with the law; or
c. information that is generated in a self-audit that documents potential law violations.

Bill Implementation:

Once a company designates documents as covered by the legislation's confidentiality provisions, does the legislation envision any review of the legitimacy of those assertions by a neutral government official?

If a company designates documents as covered by the bill, a member of the public subsequently requests the information, but the company refuses to give consent to the release of the information, what kind of recourse will be available to the requestor?

What agency or department will serve as the repository of information covered by the legislation, or may any agency or department become a repository?

Under which of the following situations is information protected by the legislation's confidentiality provisions:

a. information stamped confidential is simultaneously submitted to a federal enforcement agency and the Homeland Security Office. It later turns out that the information indicates that the company has committed civil violations of the laws enforced by the agency; or
b. information stamped confidential is submitted to the Homeland Security Office after unstamped information has been submitted to another federal enforcement agency. The enforcement agency is preparing to go to court to seek penalties for conduct documented in the documents.

Exemptions:

Would the legislation protect from disclosure information that a federal agency or department could obtain by subpoena or other legally binding information request, whether or not such a subpoena or request has been transmitted to the submitter?

If information is already in the public domain, is it still qualified for confidential treatment under the legislation?

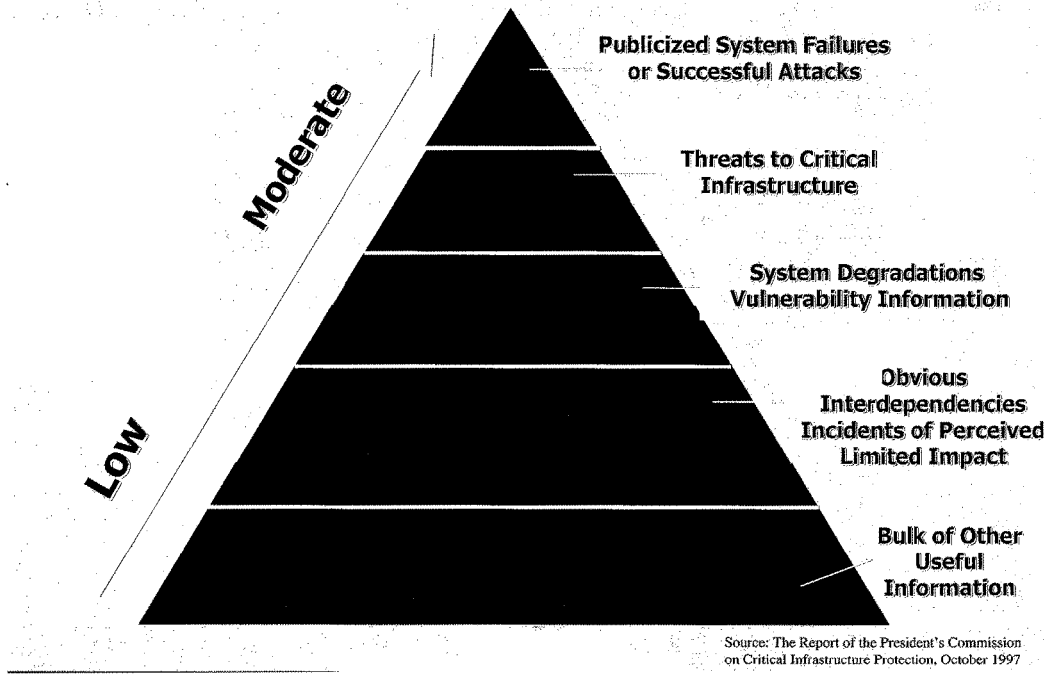
If the same type of information is – or routinely has been – in the public domain, is it still qualified for confidential treatment under the legislation?

What kinds of activities would constitute the "proper performance of official duties" by a government representative sufficient to exempt information from the protections of the bill?

"It is very important to concentrate on hitting the U.S. economy through all possible means…look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck…".

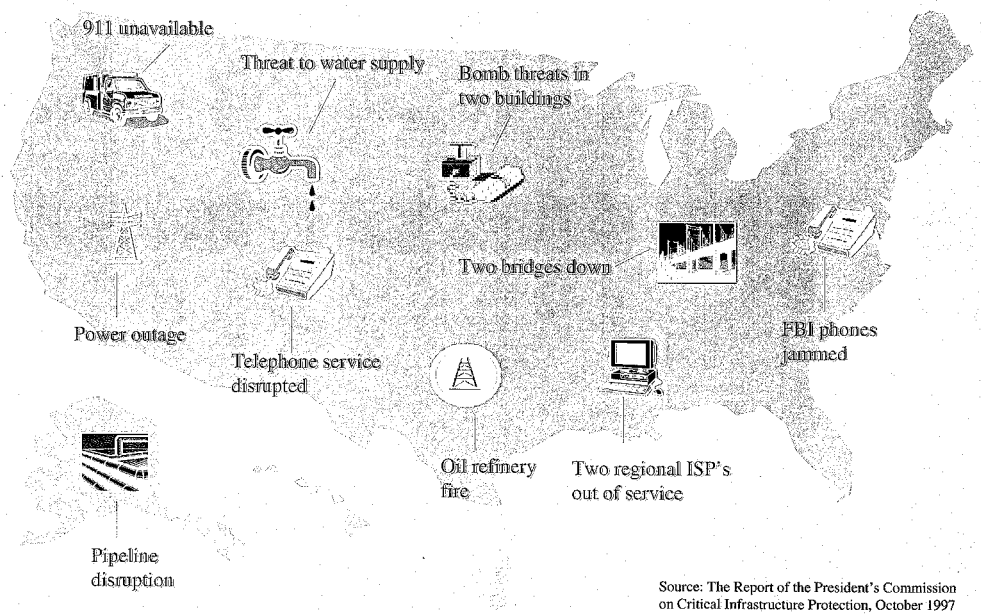
-Osama Bin Laden, December 27, 2001

Reporting and Dissemination of Information

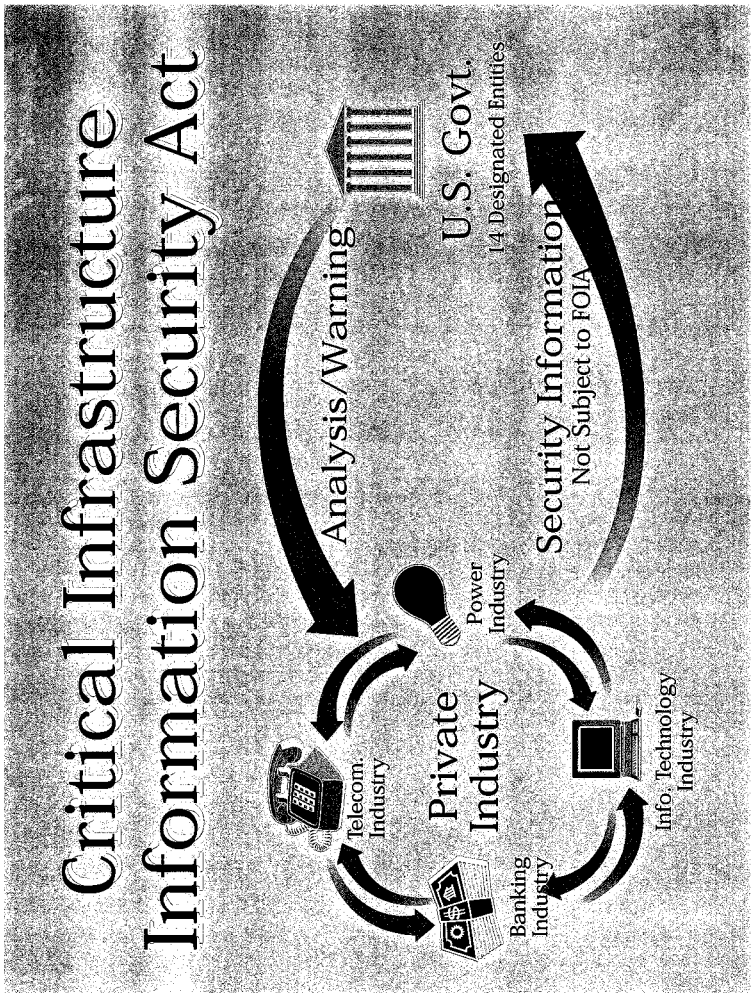


Source: The Report of the President's Commission on Critical Infrastructure Protection, October 1997

Coincidence or Attack?



Source: The Report of the President's Commission on Critical Infrastructure Protection, October 1997


Critical Infrastructure
Information Security Act
Telecom. Industry
Banking Industry
Private Industry
Power Industry
Info. Technology Industry
Analysis/Warning
Security Information
Not Subject to FOIA
U.S. Govt.
14 Designated Entities

II

107TH CONGRESS
1ST SESSION

S. 1456

To facilitate the security of the critical infrastructure of the United States, to encourage the secure disclosure and protected exchange of critical infrastructure information, to enhance the analysis, prevention, and detection of attacks on critical infrastructure, to enhance the recovery from such attacks, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 24, 2001

Mr. BENNETT (for himself and Mr. KYL) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

---

A BILL

To facilitate the security of the critical infrastructure of the United States, to encourage the secure disclosure and protected exchange of critical infrastructure information, to enhance the analysis, prevention, and detection of attacks on critical infrastructure, to enhance the recovery from such attacks, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Critical Infrastructure Information Security Act of 2001".

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The critical infrastructures that underpin our society, national defense, economic prosperity, and quality of life—including energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age.

(2) The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex global network of interconnectivity and interdependence. As a result, new vulnerabilities to such systems and infrastructures have emerged, such as the threat of physical and cyber attacks from terrorists or hostile states. These attacks could disrupt the economy and endanger the security of the United States.

(3) The private sector, which owns and operates the majority of these critical infrastructures, and the Federal Government, which has unique information and analytical capabilities, could both greatly benefit from cooperating in response to threats, vulnerabilities, and actual attacks to critical infrastructures by sharing information and analysis.

(4) The private sector is hesitant to share critical infrastructure information with the Federal Government because—

(A) Federal law provides no clear assurance that critical infrastructure information voluntarily submitted to the Federal Government will be protected from disclosure or misuse;

(B) the framework of the Federal Government for critical infrastructure information sharing and analysis is not sufficiently developed; and

(C) concerns about possible prosecution under the antitrust laws inhibit some companies from partnering with other industry members, including competitors, to develop cooperative infrastructure security strategies.

(5) Statutory nondisclosure provisions that qualify as Exemption 3 statutes under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act), many of them longstanding, prohibit disclosure of numerous classes of information under that Act. These statutes cover specific and narrowly defined classes of information and are consistent with the principles of free and open government that that Act seeks to facilitate.

(6) Since the infrastructure information that this Act covers is not normally in the public domain, preventing public disclosure of this sensitive information serves the greater good by promoting national security and economic stability.

SEC. 3. PURPOSE.

The purpose of this Act is to foster improved security of critical infrastructure by—

(1) promoting the increased sharing of critical infrastructure information both between private sector entities and between the Federal Government and the private sector; and

(2) encouraging the private sector and the Federal Government to conduct better analysis of critical infrastructure information in order to prevent, detect, warn of, and respond to incidents involving critical infrastructure.

SEC. 4. DEFINITIONS.

In this Act:

(1) AGENCY.—The term "agency" has the meaning given that term in section 551 of title 5, United States Code.

(2) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure"—

1 (A) means physical and cyber-based sys-
2 tems and services essential to the national de-
3 fense, government, or economy of the United
4 States, including systems essential for tele-
5 communications (including voice and data
6 transmission and the Internet), electrical power,
7 gas and oil storage and transportation, banking
8 and finance, transportation, water supply,
9 emergency services (including medical, fire, and
10 police services), and the continuity of govern-
11 ment operations; and
12 (B) includes any industry sector des-
13 ignated by the President pursuant to the Na-
14 tional Security Act of 1947 (50 U.S.C. 401 et
15 seq.) or the Defense Production Act of 1950
16 (50 U.S.C. App. 2061 et seq.) as essential to
17 provide resources for the execution of the na-
18 tional security strategy of the United States, in-
19 cluding emergency preparedness activities pur-
20 suant to title VI of the Robert T. Stafford Dis-
21 aster Relief and Emergency Assistance Act (42
22 U.S.C. 5195 et seq.).
23 (3) CRITICAL INFRASTRUCTURE INFORMA-
24 TION.—The term "critical infrastructure informa-
25 tion" means information related to—

(A) the ability of any protected system or critical infrastructure to resist interference, compromise, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) any planned or past assessment, projection, or estimate of the security vulnerability of a protected system or critical infrastructure, including security testing, risk evaluation, risk management planning, or risk audit;

(C) any planned or past operational problem or solution, including repair, recovery, reconstruction, insurance, or continuity, related to the security of a protected system or critical infrastructure; or

(D) any threat to the security of a protected system or critical infrastructure.

(4) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created by public or private sector organizations, and composed primarily of such organizations, for purposes of—

1 (A) gathering and analyzing critical infra-
2 structure information in order to better under-
3 stand security problems related to critical infra-
4 structure and protected systems, and inter-
5 dependencies of critical infrastructure and pro-
6 tected systems, so as to ensure the availability,
7 integrity, and reliability of critical infrastruc-
8 ture and protected systems;
9 (B) communicating or disclosing critical
10 infrastructure information to help prevent, de-
11 tect, mitigate, or recover from the effects of a
12 problem related to critical infrastructure or pro-
13 tected systems; and
14 (C) voluntarily disseminating critical infra-
15 structure information to entity members, other
16 Information Sharing and Analysis Organiza-
17 tions, the Federal Government, or any entities
18 which may be of assistance in carrying out the
19 purposes specified in subparagraphs (A) and
20 (B).
21 (5) PROTECTED SYSTEM.—The term "protected
22 system"—
23 (A) means any service, physical or com-
24 puter-based system, process, or procedure that

1 directly or indirectly affects a facility of critical
2 infrastructure; and
3 (B) includes any physical or computer-
4 based system, including a computer, computer
5 system, computer or communications network,
6 or any component hardware or element thereof,
7 software program, processing instructions, or
8 information or data in transmission or storage
9 therein (irrespective of storage medium).
10 (6) VOLUNTARY.—The term "voluntary", in the
11 case of the submittal of information or records to
12 the Federal Government, means the submittal of the
13 information or records in the absence of an agency's
14 exercise of legal submission.

15 **SEC. 5. PROTECTION OF VOLUNTARILY SHARED CRITICAL**
16 **INFRASTRUCTURE INFORMATION.**

17 (a) PROTECTION.
18 (1) IN GENERAL.—Notwithstanding any other
19 provision of law, critical infrastructure information
20 that is voluntarily submitted to a covered Federal
21 agency for analysis, warning, interdependency study,
22 recovery, reconstitution, or other informational pur-
23 pose, when accompanied by an express statement
24 specified in paragraph (3)—

(A) shall not be made available under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) may not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law, unless such information is submitted in bad faith; and

(C) may not, without the written consent of the person or entity submitting such information, be used for a purpose other than the purpose of this Act, or disclosed by any officer or employee of the United States, except pursuant to the official duties of such officer or employee pursuant to this Act.

(2) COVERED FEDERAL AGENCY DEFINED.—In paragraph (1), the term "covered Federal agency" means the following:

(A) The Department of Justice.

(B) The Department of Defense.

(C) The Department of Commerce.

(D) The Department of Transportation.

1 (E) The Department of the Treasury.
2 (F) The Department of Health and
3 Human Services.
4 (G) The Department of Energy.
5 (H) The Environmental Protection Agency.
6 (I) The General Services Administration.
7 (J) The Federal Communications Commis-
8 sion.
9 (K) The Federal Emergency Management
10 Agency.
11 (L) The National Infrastructure Protection
12 Center.
13 (M) The National Communication System.
14 (3) EXPRESS STATEMENT.—For purposes of
15 paragraph (1), the term "express statement", with
16 respect to information or records, means—
17 (A) in the case of written information or
18 records, a written marking on the information
19 or records as follows: "This information is vol-
20 untarily submitted to the Federal Government
21 in expectation of protection from disclosure
22 under the provisions of the Critical Infrastruc-
23 ture Information Security Act of 2001."; or
24 (B) in the case of oral information, a
25 statement, substantially similar to the words

1 specified in subparagraph (A), to convey that
2 the information is voluntarily submitted to the
3 Federal Government in expectation of protec-
4 tion from disclosure under the provisions of this
5 Act.

6 (b) INDEPENDENTLY OBTAINED INFORMATION.
7 Nothing in this section shall be construed to limit or other-
8 wise affect the ability of the Federal Government to obtain
9 and use under applicable law critical infrastructure infor-
10 mation obtained by or submitted to the Federal Govern-
11 ment in a manner not covered by subsection (a).

12 (c) TREATMENT OF VOLUNTARY SUBMITTAL OF IN-
13 FORMATION.—The voluntary submittal to the Federal
14 Government of information or records that are protected
15 from disclosure by this section shall not be construed to
16 constitute compliance with any requirement to submit
17 such information to a Federal agency under any other pro-
18 vision of law.

19 (d) PROCEDURES.

20 (1) IN GENERAL.—The Director of the Office of
21 Management and Budget shall, in consultation with
22 appropriate representatives of the National Security
23 Council and the Office of Science and Technology
24 Policy, establish uniform procedures for the receipt,
25 care, and storage by Federal agencies of critical in-

1 frastructure information that is voluntarily sub-
2 mitted to the Federal Government. The procedures
3 shall be established not later than 90 days after the
4 date of the enactment of this Act.

5 (2) ELEMENTS.—The procedures established
6 under paragraph (1) shall include mechanisms
7 regarding—

8 (A) the acknowledgement of receipt by
9 Federal agencies of critical infrastructure infor-
10 mation that is voluntarily submitted to the Fed-
11 eral Government, including confirmation that
12 such information is protected from disclosure
13 under this Act;

14 (B) the marking of such information as
15 critical infrastructure information that is volun-
16 tarily submitted to the Federal Government for
17 purposes of this Act;

18 (C) the care and storage of such informa-
19 tion; and

20 (D) the protection and maintenance of the
21 confidentiality of such information so as to per-
22 mit, pursuant to section 6, the sharing of such
23 information within the Federal Government,
24 and the issuance of notices and warnings re-
25 lated to protection of critical infrastructure.

SEC. 6. NOTIFICATION, DISSEMINATION, AND ANALYSIS REGARDING CRITICAL INFRASTRUCTURE INFORMATION.

(a) NOTICE REGARDING CRITICAL INFRASTRUCTURE SECURITY.

(1) IN GENERAL.—A covered Federal agency (as specified in section 5(a)(2)) receiving significant and credible information under section 5 from a private person or entity about the security of a protected system or critical infrastructure of another known or identified private person or entity shall, to the extent consistent with requirements of national security or law enforcement, notify and convey such information to such other private person or entity as soon as reasonable after receipt of such information by the agency.

(2) CONSTRUCTION.—Paragraph (1) may not be construed to require an agency to provide specific notice where doing so would not be practicable, for example, based on the quantity of persons or entities identified as having security vulnerabilities. In instances where specific notice is not practicable, the agency should take reasonable steps, consistent with paragraph (1), to issue broadly disseminated advisories or alerts.

1 (b) ANALYSIS OF INFORMATION.—Upon receipt of
2 critical infrastructure information that is voluntarily sub-
3 mitted to the Federal Government, the Federal agency re-
4 ceiving such information shall—
5 (1) share with appropriate covered Federal
6 agencies (as so specified) all such information that
7 concerns actual attacks, and threats and warnings of
8 attacks, on critical infrastructure and protected sys-
9 tems;
10 (2) identify interdependencies; and
11 (3) determine whether further analysis in con-
12 cert with other Federal agencies, or warnings under
13 subsection (c), are warranted.
14 (c) ACTION FOLLOWING ANALYSIS.
15 (1) AUTHORITY TO ISSUE WARNINGS.—As a re-
16 sult of analysis of critical infrastructure information
17 under subsection (b), a Federal agency may issue
18 warnings to individual companies, targeted sectors,
19 other governmental entities, or the general public re-
20 garding potential threats to critical infrastructure.
21 (2) FORM OF WARNINGS.—In issuing a warning
22 under paragraph (1), the Federal agency concerned
23 shall take appropriate actions to prevent the disclo-
24 sure of the source of any voluntarily submitted crit-

1 ical infrastructure information that forms the basis
2 for the warning.
3 (d) STRATEGIC ANALYSES OF POTENTIAL THREATS
4 TO CRITICAL INFRASTRUCTURE.
5 (1) IN GENERAL.—The President shall des-
6 ignate an element in the Executive Branch—
7 (A) to conduct strategic analyses of poten-
8 tial threats to critical infrastructure; and
9 (B) to submit reports on such analyses to
10 Information Sharing and Analysis Organiza-
11 tions and such other entities as the President
12 considers appropriate.
13 (2) STRATEGIC ANALYSES.
14 (A) INFORMATION USED.—In conducting
15 strategic analyses under paragraph (1)(A), the
16 element designated to conduct such analyses
17 under paragraph (1) shall utilize a range of
18 critical infrastructure information voluntarily
19 submitted to the Federal Government by the
20 private sector, as well as applicable intelligence
21 and law enforcement information.
22 (B) AVAILABILITY.—The President shall
23 take appropriate actions to ensure that, to the
24 maximum extent practicable, all critical infra-
25 structure information voluntarily submitted to

1 the Federal Government by the private sector is
2 available to the element designated under para-
3 graph (1) to conduct strategic analyses under
4 paragraph (1)(A).
5 (C) FREQUENCY.—Strategic analyses shall
6 be conducted under this paragraph with such
7 frequency as the President considers appro-
8 priate, and otherwise specifically at the direc-
9 tion of the President.
10 (3) REPORTS.
11 (A) IN GENERAL.—Each report under
12 paragraph (1)(B) shall contain the following:
13 (i) A description of currently recog-
14 nized methods of attacks on critical infra-
15 structure.
16 (ii) An assessment of the threats to
17 critical infrastructure that could develop
18 over the year following such report.
19 (iii) An assessment of the lessons
20 learned from responses to previous attacks
21 on critical infrastructure.
22 (iv) Such other information on the
23 protection of critical infrastructure as the
24 element conducting analyses under para-
25 graph (1) considers appropriate.

1 (B) FORM.—Reports under this paragraph
2 may be in classified or unclassified form, or
3 both.
4 (4) CONSTRUCTION.—Nothing in this sub-
5 section shall be construed to modify or alter any re-
6 sponsibility of a Federal agency under subsections
7 (a) through (c).
8 (e) PLAN FOR STRATEGIC ANALYSES OF THREATS
9 TO CRITICAL INFRASTRUCTURE.
10 (1) PLAN.—The President shall develop a plan
11 for carrying out strategic analyses of threats to crit-
12 ical infrastructure through the element in the Exec-
13 utive Branch designated under subsection (d)(1).
14 (2) ELEMENTS.—The plan under paragraph (1)
15 shall include the following:
16 (A) A methodology for the work under the
17 plan of the element referred to in paragraph
18 (1), including the development of expertise
19 among the personnel of the element charged
20 with carrying out the plan and the acquisition
21 by the element of information relevant to the
22 plan.
23 (B) Mechanisms for the studying of
24 threats to critical infrastructure, and the
25 issuance of warnings and recommendations re-

1 garding such threats, including the allocation of
2 personnel and other resources of the element in
3 order to carry out those mechanisms.
4 (C) An allocation of roles and responsibil-
5 ities for the work under the plan among the
6 Federal agencies specified in section 5(a)(2), in-
7 cluding the relationship of such roles and re-
8 sponsibilities.
9 (3) REPORTS.
10 (A) INTERIM REPORT.—The President
11 shall submit to Congress an interim report on
12 the plan developed under paragraph (1) not
13 later than 120 days after the date of the enact-
14 ment of this Act.
15 (B) FINAL REPORT.—The President shall
16 submit to Congress a final report on the plan
17 developed under paragraph (1), together with a
18 copy of the plan, not later than 180 days after
19 the date of the enactment of this Act.

20 **SEC. 7. ANTITRUST EXEMPTION FOR ACTIVITY INVOLVING**
21 **AGREEMENTS ON CRITICAL INFRASTRUC-**
22 **TURE MATTERS.**

23 (a) ANTITRUST EXEMPTION.—The antitrust laws
24 shall not apply to conduct engaged in by an Information
25 Sharing and Analysis Organization or its members, includ-

1 ing making and implementing an agreement, solely for
2 purposes of—
3 (1) gathering and analyzing critical infrastruc-
4 ture information in order to better understand secu-
5 rity problems related to critical infrastructure and
6 protected systems, and interdependencies of critical
7 infrastructure and protected systems, so as to en-
8 sure the availability, integrity, and reliability of crit-
9 ical infrastructure and protected systems;
10 (2) communicating or disclosing critical infra-
11 structure information to help prevent, detect, miti-
12 gate, or recover from the effects of a problem related
13 to critical infrastructure or protected systems; or
14 (3) voluntarily disseminating critical infrastruc-
15 ture information to entity members, other Informa-
16 tion Sharing and Analysis Organizations, the Fed-
17 eral Government, or any entities which may be of as-
18 sistance in carrying out the purposes specified in
19 paragraphs (1) and (2).
20 (b) EXCEPTION.—Subsection (a) shall not apply with
21 respect to conduct that involves or results in an agreement
22 to boycott any person, to allocate a market, or to fix prices
23 or output.
24 (c) ANTITRUST LAWS DEFINED.—In this section, the
25 term "antitrust laws"—

1 (1) has the meaning given such term in sub-
2 section (a) of the first section of the Clayton Act (15
3 U.S.C. 12(a)), except that such term includes sec-
4 tion 5 of the Federal Trade Commission Act (15
5 U.S.C. 45) to the extent such section 5 applies to
6 unfair methods of competition; and
7 (2) includes any State law similar to the laws
8 referred to in paragraph (1).

9 **SEC. 8. NO PRIVATE RIGHT OF ACTION.**

10 Nothing in this Act may be construed to create a pri-
11 vate right of action for enforcement of any provision of
12 this Act.

○

WASHINGTON NATIONAL OFFICE
Laura W. Murphy
Director

122 Maryland Avenue, NE, Washington, D.C. 20002 **Tel** (202) 544-1681 **Fax** (202) 546-0738

June 5, 2002

Hon. Joseph I. Lieberman
Chairman
Senate Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

Hon. Fred Thompson
Ranking Member
Senate Governmental Affairs Committee
605 Hart Senate Office Building
Washington, DC 20510

Re: Statement for the Record Concerning Public-Private Information Sharing and Critical Infrastructure Security

Dear Chairman Lieberman and Senator Thompson:

On behalf of the American Civil Liberties Union (ACLU) and its approximately 300,000 members, we welcome this opportunity to discuss proposals for information sharing between the public and private sectors with respect to critical infrastructure systems. We commend you for examining these issues in a hearing before your committee on May 8, and we ask that this submission be made a part of the record of that hearing.

The ACLU is a non-partisan, non-profit organization dedicated to preserving the principles of our constitutional democracy, including open and accountable government. We support legislative and administrative efforts to encourage greater information sharing about cyber-vulnerabilities in critical infrastructure systems, such as electricity grids, banking systems, and water systems. Such efforts are needed in order to ensure that critical systems are made secure from hackers and others who desire to do harm to the United States and its economy.

However, the ACLU strongly opposes proposals[1] to create a broad new exemption to the Freedom of Information Act (FOIA), 5 U.S.C. § 552 for information that companies

[1] Two bills that contain broad FOIA exemptions for "critical infrastucture" or "cyber-security" information are currently pending in the House and Senate: S. 1456, the Critical Infrastructure Information Security Act of 2001 and H.R. 2435, the Open Government and the Cyber Security Information Act. Recently, during markup of another, unproblematic critical infrastructure bill, S. 1989, an amendment was offered to enact FOIA exemption language. The amendment was withdrawn.

Nadine Strossen *President* **Anthony D. Romero** *Executive Director* **Kenneth B. Clark** *Chair, National Advisory Council* **Richard Zacks** *Treasurer*
National Headquarters 125 Broad Street, New York, NY 10004-2400 (212) 549-2500

provide about their "critical infrastructure" systems. The FOIA is the bedrock statute designed to preserve openness and accountability in government and new exemptions to its provisions should not be created lightly.

Last year, special interest efforts to add a "critical infrastructure" exemption to the FOIA, without debate and without adequate consideration, were wisely shelved. Yet, following intense industry lobbying, these proposals have now been revived, even though:

- There is a virtual consensus in government and industry, even among supporters of a critical infrastructure exemption, that the current FOIA exemptions are sufficient to protect any confidential information about critical infrastructure that is voluntarily shared with the government.

- There is little confidence that creating a new exemption would be effective in encouraging greater information sharing, because many experts, including many industry experts, believe that to the extent companies are choosing not to share such information, it is for reasons other than a (wholly unfounded) fear of disclosure under the FOIA.

- Current proposals to create a new FOIA exemption are overbroad because they would protect not only those responsible corporate citizens who are attempting to address a vulnerability, but could shield both government and industry from scrutiny even if they fail to do anything to fix the problem.

This last concern is not theoretical. Earlier this year in Israel, the media obtained a government report that discussed the vulnerability of a fuel depot to terrorists. Military censors blocked publication of the report, and persuaded the mayor of Tel Aviv not to go public with a campaign to fix the problem. Nothing was done. Terrorists then attacked the fuel depot. In that case, public debate might well have forced action to address the problem.[2] Likewise, Soviet secrecy concerning its nuclear weapons program has hindered efforts to account for all of its nuclear missiles, seriously increasing the risk that terrorists will succeed in acquiring such weapons.

All too often, secrecy simply provides a shield for public and private incompetence. We are convinced that security and liberty need not be at odds.

The Freedom of Information Act: Essential to an Accountable Democracy

The FOIA is the bedrock statute that preserves government accountability by requiring government agencies to disclose information to requesters in a timely manner. The basic open government policy of the FOIA has worked well since the statute's enactment and has served as a model for both state and foreign governments' open records laws. As the Supreme Court has made clear, "Disclosure, not secrecy, is the dominant objective of the Act."[3]

---

[2] *See* Aviv Lavie, *Media: Sensing the Censor*, Ha'aretz (Tel Aviv, Israel), May 29, 2002.
[3] *Department of the Air Force* v. *Rose*, 425 U.S. 352 (1976).

The disclosure of information pursuant to the FOIA has for over three decades helped citizens protect the health and safety of their communities against environmental hazards. Of course, while certain information that is highly sensitive can and should be kept from public view, one cannot safely assume that is the case whenever the government invokes "terrorism." For example, disclosure laws, including the FOIA, have helped ACLU and other civil rights organizations obtain information about abusive government practices, such as arbitrary arrests and secretive detentions, information of vital interest to the public.

Since the attacks of September 11, 2001, a number of steps have been taken, many without adequate deliberation, to increase government secrecy and to reduce public access to government records.[4] As with other proposals that negatively impact civil liberties, many of these new policies have been proposed more out of a desire to take advantage of the public's fears of terrorism than from a genuine desire to make America safer. A sober second look has proven many to be unnecessary.

For example, both President Bush's executive order restricting access to presidential records and Attorney General Ashcroft's ill-advised memorandum discouraging agencies from releasing information under the FOIA have now been firmly rejected, on a bipartisan basis, by Chairman Burton and Ranking Member Waxman, of the House Government Reform Committee.

At the state level, a number of proposals have been advanced to weaken open records laws. In Florida, for example, over 160 proposals were advanced earlier this year to create new exemptions to that state's strong open records policy, embodied in its state constitution. Following a public outcry and after taking the time to deliberate, only a handful were enacted, and the legislature agreed to submit to the voters a proposal to require a two thirds vote of each chamber before any new exemptions are created.

Open government is a core American value. It should not be set aside for reasons other than genuine necessity.

Congress should ask three questions before enacting any proposed exemption. First, is a new exemption necessary? Second, will it work (i.e., will it actually encourage greater information sharing)? Third, will it backfire (e.g., by allowing companies and the government to hide their failures)?

Is a New Exemption Necessary?

If a proposed exemption for critical infrastructure information is not necessary, it should not be adopted out of a misguided effort to reassure private sector submitters that already exempt information "really" is exempt from disclosure. The FOIA is simply too

[4] For an overview, see *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know,* Reporters Committee for Freedom of the Press (March 2002), available at http://www.rcfp.org/news/documents/Homefront_Confidential.pdf.

important to the functioning of our democracy and accountability in government for exemptions to its provisions to be created for symbolic, rather than substantive, reasons.

The FOIA already contains a number of common sense exemptions that would cover critical infrastructure information the disclosure of which could result in harm. The FOIA does not require the disclosure of national security information (exemption 1), sensitive law enforcement information (exemption 7), or confidential business information (exemption 4).

Courts have carefully weighed the public's need for disclosure against the possible harms of disclosure under FOIA's traditional exemptions. In deciding whether to disclose technical information voluntarily submitted by private industry, courts have given substantial – many in the public interest and FOIA requester community would say excessive – deference to industry demands for confidentiality of business information under exemption 4.

Generally, information that a business voluntarily submits to the government on the basis that it be kept confidential is already exempt from disclosure if the company does not customarily release such information to the public and preserving confidentiality is necessary to ensure that the government will continue to receive industry's cooperation. *See, e.g., Critical Mass Energy Project* v. *Nuclear Regulatory Commission*, 975 F.2d 871 (D.C. Cir. 1992). It is difficult to see how any truly sensitive business information that was voluntarily submitted by a company concerning the vulnerabilities of its critical infrastructure could be released under this standard.

Indeed, supporters of a new FOIA exemption have, when pressed, been forthright in admitting that such legislation simply is not needed to protect sensitive information from disclosure. For example,

- Senator Bennett, chief sponsor of the FOIA exemption legislation, has admitted that "[t]he Freedom of Information Act itself" currently allows sensitive information to be protected. "That is, there are provisions in the Act that say information need not be shared" with the public.[5]

- John S. Tritak, Director of the Critical Infrastructure Assurance Office of the U.S. Chamber of Commerce, says "You could say that [in the] current environment, if you're very careful and you watch out, the old existing exemptions will cover any concerns that may arise under FOIA, not to worry."[6]

- Ronald L. Dick, Director of the National Infrastructure Protection Center of the Federal Bureau of Investigation (FBI), has said "[M]any legal authorities have

[5] *Senate Governmental Affairs Committee Holds Hearing on Private and Public Information Sharing and Infrastructure Security* (FDCH Transcripts), May 8, 2002.
[6] *Id.*

agreed that the federal government has the ability to protect information from mandatory disclosure under the current statutory framework."[7]

- VeriSign public policy director Michael Aisenberg has said worries about disclosure were overblown because FOIA already protects sensitive information, and new legislation is simply not needed "substantively."[8]

Rather than put forward evidence that some information about critical infrastructure exists that is not adequately protected, supporters of a new exemption have said "it doesn't matter" whether current law provides adequate protection. Rather, it is said, a new exemption is needed because of a "perception" in private industry that there is some risk, however remote, that information that is voluntarily submitted to the government might be at risk of disclosure under FOIA.

If industry is unwilling to provide information to the government, despite adequate legal protection, the solution is not to change the law but to change the misperception by issuing legal guidance making clear the parameters of the FOIA as it currently exists. If a misperception exists that truly sensitive information that is given to the government cannot be protected from disclosure, it is hard to see how that will change if another exemption is enacted.

Would a New Exemption Actually Facilitate Greater Information Sharing?

There is a consensus that while much information is shared between industry and government concerning the vulnerabilities of their systems to cyber-attacks, more needs to be done. For example, much has been made of the fact that while 90% of respondents to an FBI survey on computer crime said they had security breaches, only 34% of these were reported to law enforcement.[9]

Fear of adverse publicity and its effect on a company's image undoubtedly plays a role in companies' reluctance to come forward. Yet there is no evidence that the reason for such reluctance is fear of disclosure of such information *under the FOIA*. Indeed, there is much reason for skepticism that FOIA plays any substantial role in causing industry to hesitate in reporting cyber-attacks to the government.

After all, if a company does report a cyber-attack to law enforcement, the company knows such a report could result in a prosecution in open court, revealing at the least the fact that an attack occurred and at most substantial technical details the company would prefer to keep secret. Law enforcement officials make clear that a number of factors result in industry reluctance to report cyber-attacks. Chief among these are "concerns

---

[7] *Id.*
[8] *Washington Internet Daily*, April 18, 2002
[9] These figures were reported as part of the annual Computer Security Institute/FBI Computer Crime and Security Survey, released in April 2002. *Statement for the Record of Ronald K. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, on Critical Infrastructure Information Sharing Before the Senate Committee on Governmental Affairs*, May 8, 2002.

about whether the Justice Department would pursue prosecutions at the expense of private sector business interest[s]."[10]

Again, industry sources themselves make this clear:

- Alan Paller, Director of Research, the SANS Institute says quite simply, "[A] clarification of the FOIA exemption is *not going to cause companies to share cyber attack data with the government* . . . . [E]ven if you provide a perfect FOIA exemption, the companies under attack are unlikely to share the data."[11]

- John S. Tritak of the U.S. Chamber of Commerce: "I don't think we're going to solve this problem . . . with a passage of legislation . . . You're not going to get an avalanche of information being shared with the government just because you have this." [12]

- Harris N. Miller of the Information Technology Association of America: "[W]e all remember the old adage, Macy's doesn't tell Gimble's . . . . And particularly Macy's and Gimble's don't go tell the cops."[13]

If there is a consensus that (1) a new exemption is not necessary "substantively," and (2) a new exemption would not be effective in causing companies to share information they are currently reluctant to share, why risk it? Why risk the chance that a new exemption would allow important information that the public should have a right to know be made secret so that industry and government can evade accountability?

Would a New Exemption Backfire, By Hiding the Need for Corrective Action?

Creating an overbroad exemption for "critical infrastructure information" would undermine, rather than enhance, security. Such an exemption would permit private industry and the government to shield from the public the actions they are taking - and, more importantly, the actions they are not taking - to protect the public from attacks on critical infrastructures.

It would obviously be counterproductive for government to shield information currently subject to public scrutiny if such scrutiny would prod companies and the government to take corrective action. As the examples of the Israeli fuel dump and the Soviet Union's potential "loose nukes" demonstrate, such incentives are vital to protecting our nation's security.

---

[10] Ronald K. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, *Senate Governmental Affairs Committee Holds Hearing on Private and Public Information Sharing and Infrastructure Security* (FDCH Transcripts), May 8, 2002.
[11] *Senate Governmental Affairs Hearing, supra..*
[12] *Id.*
[13] *Id.*

Supporters of an exemption often cite the example of legislation adopted to deal with the "Y2K" computer problem, which also contained an exemption and is said to have worked well. This example of a discrete, widely known computer problem simply shows why a broader exemption would not work. Put simply, everyone knew about the Y2K problem, and there was enormous public pressure to fix non-compliant computer systems before it was too late. The proposed legislation, however, does not provide a FOIA exemption merely for information about how a specific widely-known problem – with a natural and inexorable time limit – might be fixed, but permits the very fact that a vulnerability exists to be kept secret indefinitely. Such secrecy undercuts the very incentive – public pressure – that worked so well to encourage efforts to fix Y2K before it was too late.

For the all of the above reasons, ACLU opposes the enactment of a new FOIA exemption for critical infrastructure information. At the very least, however, any new exemption that Congress enacts should be subject to the following responsible limits:

First, any new exemption must be limited to clearly marked cyber-security documents, i.e., reports that describe cyber-attacks on a company's computer systems that have resulted or could result in some harm to its critical infrastructure. It should not apply to information about *all* vulnerabilities in critical infrastructure. Proposals to exempt information that is voluntarily shared with the government were developed to deal with the discrete and relatively new problem of cyber-attacks. To expand the scope of information that is exempted to include information about vulnerabilities to traditional physical attacks would interfere with a host of environmental and public safety regulatory regimes that have been developed over decades.

Second, any new exemption must be for written documents only, not "information" of all sorts. It would be virtually impossible to determine if information possessed by the government was the result of some oral conversation with a private sector company, making a FOIA exemption that covered such information unworkable and potentially devastating to the public's right to know.

Third, any new exemption must be limited in time, and should last for months, not years. A company which controls infrastructure that is vital to the public must have an incentive not only to share information, but also to do something to make itself less vulnerable to such attacks. A time limited exemption will give responsible companies and government agencies an incentive to fix their problem with due speed. Without a time limit, companies and the government can simply sit on the problem without any pressure to act.

Fourth, a new exemption should be an alternative to existing FOIA protections, not a new club to wield against FOIA requesters. Companies that wish to take advantage of the new exemption should clearly state on the relevant document they are requesting confidentiality under that exemption. Companies that fail to fix their vulnerabilities within a reasonable time limit, even with the protection of the new exemption, should not be allowed to take advantage of FOIA's other potentially applicable exemptions to cover up their failure to act after that time limit has expired. If companies believe the

information they desire to share is protected under another FOIA exemption, they should be required instead to rely on that other exemption at the time of submission.

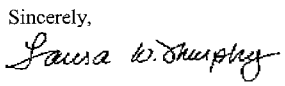
Finally, strict reporting requirements and a sunset clause should be included in the legislation to determine whether the new regime is working.

Conclusion

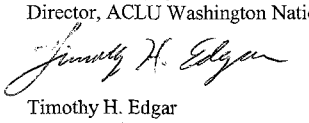
It is well known that many computer systems that control infrastructure that is vital to America's national and economic security have significant vulnerabilities. The threat of cyber-terrorism is very real. Nevertheless, Congress must tread cautiously as it considers wide-ranging proposals that could have unintended consequences for civil liberties and the public's right to know and could actually undermine, rather than enhance security.

We urge Congress to reject proposals to create yet another FOIA exemption because they are not needed, would not facilitate greater information sharing, and could actually undermine security. Even supporters concede that current law already exempts sensitive information from disclosure. Furthermore, disclosure under the FOIA is simply not the primary reason companies have been reluctant at times to report cyber-attacks to the government. Finally, if Congress is intent on pressing forward, we strongly urge responsible limits on any such exemption to make sure it protects companies that are doing what they must to fix their vulnerabilities, rather than shielding public and private incompetence from view.

Sincerely,



Laura W. Murphy
Director, ACLU Washington National Office



Timothy H. Edgar
ACLU Legislative Counsel

JOHN P. CONNELLY
VICE PRESIDENT, MEMBER RELATIONS
AND CORPORATE SECRETARY

May 15, 2002

The Honorable Joseph Lieberman
Chairman
Committee on Governmental Affairs
340 Senate Dirksen Office Bldg.
Washington, DC 20510-6250

Re: Statement of the American Chemistry Council on Securing our Infrastructure: Private/Public Information Sharing

Dear Chairman Lieberman:

The American Chemistry Council commends you for holding last week's hearing on the important subject of sharing information about critical infrastructure. We also appreciate your willingness to hold the record open for a week so that organizations such as ours could be heard on this vital topic. We strongly urge you to move as quickly as possible to report out S. 1456 in substantially the form of the Bennett/Kyl/Davis/Moran staff draft, so that such information sharing can be promoted by reasonable legal protections. We also urge you to supplement the bill to facilitate the issuance of more security clearances to employees of critical infrastructure companies.

The American Chemistry Council represents over 95% of domestic productive capacity in the business of chemistry. Our industry underlies virtually every sector of the nation's critical infrastructure and is therefore equally critical. The products of chemistry are also key to our national defense (e.g., composite alloys, bullet-resistant glass, fire-retardant clothing, bulletproof fibers) and our health care system (e.g., pharmaceuticals, catheters, stethoscope diaphragms, oxygen tents, syringes, surgical instruments, clear IV components and kidney dialysis filters). It is obviously essential that companies in the business of chemistry be able to share information among themselves and with the federal government to ensure that these essential products continue to be available to Americans.

Since September 11, our industry has coordinated closely on security issues with the Office of Homeland Security, the FBI, the National Security Council, the Critical Infrastructure Assurance Office and the Critical Infrastructure Protection Board, as well as with regulatory agencies such as DOT, EPA and OSHA. Most important for the Committee's purposes, on April 24 our president and Ronald Dick, Director of the National Infrastructure Protection Center (NIPC), signed an agreement establishing a Chemical Sector Information Sharing and Analysis Center (ISAC). In Mr. Dick's words,

"[s]ince the chemical industry is a key component of our national infrastructure, any terrorist act that might delay distribution of these vital products, or attempt to misuse them, could compromise almost any sector of the American economy and the public safety. The chemical industry is to be commended for forming an ISAC to help enhance our nation's security."

We are moving quickly to make the Chemical Sector ISAC operational and to recruit participants. Yet we know now that the amount of information companies are willing to provide the NIPC will be inherently limited by the lack of full assurance that the information will be protected from disclosure under the Freedom of Information Act (FOIA). Also, the ability of the ISAC to become a forum for information analysis, whether among industry members or between industry and government, will be impeded by concerns that participants may be seen as running afoul of the antitrust laws, or that governmental participation may trigger the Federal Advisory Committee Act. Finally, we believe information sharing would be best enhanced by limited liability protection. The balance of this statement explains these concerns at greater length. It also explains why the federal government should establish a program to ensure that every critical infrastructure company has the ability to have an employee with a security clearance.

The Need for a Freedom of Information Act Exemption

As the hearing made clear, the single greatest obstacle to effective information sharing from the private sector to government is the absence of clear-cut assurance that this information will not be disclosed under FOIA. All the government witnesses -- even the Justice Department -- agreed that "we need to address the concerns" of critical infrastructure companies on this issue.[1]

This is not merely a matter of perception. It is true that much critical infrastructure information is confidential business information (CBI), and if voluntarily supplied to the government should be protected by FOIA Exemption 4, as construed by the D.C. Circuit's en banc holding in the *Critical Mass* case.[2] On the other hand:

- As Mr. Malcolm's written testimony noted, this decision is binding only in the D.C. Circuit.[3] Courts in other federal circuits may reach different conclusions.
- Federal agencies, including historically the Justice Department, have interpreted the decision narrowly. For example, the DOJ has issued guidance regarding the decision, "the net effect" of which - according to DOJ -- "is that most submissions considered by agencies under Exemption 4 will be considered to be

---

[1] Written statement of John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Justice Department, at 9.
[2] *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992).
[3] Malcolm statement, *supra* note 1, at 7.

'required' and so will not qualify for the broader protection afforded to 'voluntary' submissions under *Critical Mass*."[4]

- Almost a decade after *Critical Mass* was handed down, most federal agencies – including EPA -- still have not revised their FOIA rules to implement it.[5]
- Exemption 4 is discretionary – while it exempts information from mandatory disclosure under FOIA, it still leaves agencies free to disclose that information discretionarily (unless the information is a trade secret covered by the Trade Secrets Act and thus protected under Exemption 3).

Most important, there may well be some critical infrastructure information that is not CBI (and thus would fall outside Exemption 4), but which still needs to be kept confidential for reasons of national security and public safety. For example, Company A might have information about Company B's vulnerability that, if released publicly and exploited by a terrorist, might not injure Company A, but could still result in serious harm to others. Critical infrastructure information really is national security information – but the FOIA process requires affirmative classification before information can be withheld on that basis.

Presumably, vulnerability information that terrorists could exploit, once provided to the FBI or another agency tasked with homeland security duties, becomes "information compiled for law enforcement purposes" the disclosure of which "could reasonably be expected to endanger the life of physical safety of any individual" – namely, any person who could be harmed by the resulting attack. Under these circumstances, FOIA Exemption 7(F) should apply. But there is even less case law on this exemption, and again its exercise is discretionary to the relevant agency. In the end it, too, is unreliable.

For all these reasons, ACC strongly supports the approach of S. 1456 – an independent statutory requirement for protection, to be implemented via FOIA Exemption 3. Such legislation is crucial to the ability of the government to gain access to information that it otherwise may never see. We also believe the scope of the S. 1456 exemption – i.e., the definition of "critical infrastructure information" -- is appropriately narrow.

One of the public interest witnesses at the hearing suggested that any FOIA exemption be time-limited. ACC strongly opposes this concept. Much of the critical infrastructure information our members are likely to submit will be information about physical assets, rather than cyber systems. This sort of vulnerability information may remain sensitive

---

[4] DOJ, *Freedom of Information Act Guide and Privacy Act Overview* 174 (May 2000).

[5] For example, EPA has twice proposed to do so, but has never taken final action. *See* 65 Fed. Reg. 80396 (Dec. 21, 2000), 65 Fed. Reg. 52686 (Aug. 30, 2000). Moreover, under these proposals "[s]ubmissions that are required to realize the benefits of a voluntary program are considered to be mandatory" and hence not covered by *Critical Mass*. *Id* at 80396. ACC is concerned that federal agencies might consider the benefits of participating voluntarily in an ISAC to render submission of information via the ISAC to be "required."

for so long as the asset remains in its location, which could be many decades. There is simply no reasonable way to pick an appropriate time length for these purposes.

The public interest witnesses also raised the specter that submission of information falling within the proposed FOIA exemption could somehow exempt regulated entities from reporting or otherwise providing that information to government or the public where required by law. ACC is frankly baffled at how anyone could reach such a conclusion in light of the savings clauses in subsections 5(c) & (d) of the bill. Nonetheless, ACC would not oppose a clarifying statement that submission of information subject to the bill would not exempt the submitting person from any applicable obligation to report such information to a governmental entity.

The Need for Protection from Potential Antitrust Liability

ACC member company staff have been well-trained by company counsel to avoid participating in any discussions that begin to smack of antitrust. As a result, members of our industry are going to be uneasy or unwilling to engage in analysis of other companies' critical infrastructure information. This reticence, while founded in good compliance training, will seriously impair the ability of the Chemical Sector ISAC to provide a forum for information analysis, particularly in the areas of planning for response, recovery and reconstitution. The same concerns affect other critical infrastructure sectors. As a result, the owners of the great bulk of this nation's critical infrastructure are going to be very reluctant to talk about:

- Suppliers of software or other third parties whose products or services have posed or exacerbated a vulnerability; or
- How to assure supply of a critical product or service if one or more suppliers is shut down by a terrorist action.

At the hearing, Mr. Malcolm of the Justice Department expressed a willingness to look again at whether the business review letter (BRL) process is adequate for these purposes. ACC appreciates that willingness, because we feel the BRL process, as currently constituted, is not adequate:

- ACC anticipates that hundreds, perhaps thousands of entities will participate in the Chemical Sector ISAC – for there are tens of thousands of businesses in our sector. The membership of the ISAC may well change daily as companies join or drop out. However, DOJ's BRL rules require that "*[a]ll parties* requesting the review letter" provide information to it, and state clearly that the letter "shall have *no* application to *any* party which does not join in the request therefor."[6] The current BRL process does not appear to work for the ISAC that we are developing.
- A BRL "states only the enforcement intention of the [Antitrust] Division as of the date of the letter, and the Division remains completely free to bring whatever action or proceeding it subsequently comes to believe is required by the public

[6] 28 C.F.R. § 50.6 (emphasis added).

interest."[7] This is not the sort of firm, enduring commitment that businesses seek before they embark on a course of conduct that raises the prospect of antitrust liability.

ACC therefore favors the antitrust exemption offered by S. 1456. We note that it is also appropriately narrow, particularly since it retains liability for "conduct that involves or results in an agreement to boycott any person, to allocate a market, or to fix prices or output." Such an exemption is hardly an invitation to collude without sanctions. We also note that essentially the same exemption was contained in the Year 2000 Information and Readiness Disclosure Act,[8] and produced no problems that we are aware of.

The Need for a Federal Advisory Committee Act Exemption

One of S. 1456's primary goals is to "encourag[e] the private sector and the Government to conduct and share the results of better analyses of critical infrastructure information." By definition, that information is highly sensitive and needs to be secure and protected to ensure that the enemies of our society do not use it to target their assaults all the more effectively. As noted before, critical infrastructure information is really about national security, public safety, and associated threats and vulnerabilities. As such, it is precisely the sort of information whose availability should not be advertised via Federal Register notices and which should not be made available to any member of the public. Yet these are exactly what would happen if the Federal Advisory Committee Act (FACA) were to be held to apply to meetings of private and federal personnel to discuss critical infrastructure protection. Accordingly, S. 1456 properly exempts communication of critical infrastructure information to the government from FACA. The Committee should retain this exemption.

Liability Protection

It is conceivable that the critical infrastructure information that a regulated company provides to the government might also indicate that the company had violated an applicable law or regulation. More commonly, companies who believe they have complied with applicable laws and rules may be reluctant to provide the government with information that might be interpreted to mean otherwise. ACC believes that the purposes of the bill would be best served if the Committee retained the limited liability protections contained in S. 1456. As the Justice Department witness indicated, the current provisions are quite limited – they do not protect against criminal prosecution, they do not impair indirect use of information, and they allow the use of otherwise-obtained information. Again, similar protections were contained in the Year 2000 Information and Readiness Disclosure Act and led to no reported abuses. Indeed, a third or more of the states have enacted "audit immunity" legislation – in which

---

[7] *Id.* (emphasis added).
[8] Pub. L. No. 105-271, § 5, 15 U.S.C. § 1 Note.

companies are enabled to provide the government with information relating to *admitted* violations - and yet the parade of horribles predicted by opponents has never occurred. The far more modest provisions of S. 1456 - involving information that may only tangentially bear on compliance -- should pose no substantial concerns.

The "Trusted Professsional" Concept -- Every Critical Infrastructure Company Should Be Able to Have an Employee with a Security Clearance

The first thing critical infrastructure needs, according to the oral testimony of Mr. Gent of the North American Electric Reliability Council, is more security clearances for employees of critical infrastructure companies. ACC could not agree more strongly.

While ACC has worked closely and well with the FBI and other national security and law enforcement agencies since 9/11, we have been frustrated by the government's tendency to maintain a great deal of threat information under security classification. This frustration is exacerbated by the fact that many of our member companies do not have any personnel with security clearances. As a result, the FBI is reluctant to share detailed threat information with them. A system of previously vetted, "trusted professionals" within our member companies would greatly improve communications flow.

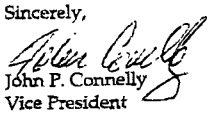
One way to develop such trusted professionals would be to establish a "National Security Academy" for those identified security professionals in critical infrastructure sectors. The training program would be similar in design and function to the FBI's National Academy for senior law enforcement personnel. This type of national security academy would provide a cadre of vetted industry professionals with security clearances and offer an extensive, two-way communication system.

ACC looks forward to working with the Committee to explore how this important recommendation could be implemented.

Conclusion

ACC thanks you for convening last week's hearing and for your willingness to move S. 1456 promptly. We strongly urge the Committee to proceed to markup and to report out S. 1456 in substantially the form of the current staff draft. We stand ready to assist the Committee in any way we can. Please feel free to contact Jamie Conrad at 703-741-5166 or Robert Flagg at 703-741-5903.

Sincerely,



John P. Connelly
Vice President
Security Team Leader

STATEMENT

OF

CATHERINE A. ALLEN, CEO
BITS
THE TECHNOLOGY GROUP
FOR
THE FINANCIAL SERVICES ROUNDTABLE

Thank you for the opportunity to submit testimony.

BITS is a not-for-profit industry consortium and a sister organization to The Financial Services Roundtable. BITS and the Roundtable's membership is comprised of the largest integrated financial services companies in the US. BITS is not a lobbying organization; instead, we serve as a business and technology strategy consortium.

As representative companies of the nation's financial services critical infrastructure, our members believe that protecting our customers' assets and focusing on reliability of services are crucial to the orderly functioning of the economy. Our systems are robust to protect against natural disasters and other sources of potential interruption of services, so we have redundant or back-up facilities. Nonetheless, we can never be 100% protected from attack. Therefore, it makes sense that the leading financial institutions work cooperatively with each other and the government to protect critical infrastructure.

To address these issues, the financial services industry formed the Financial Services Information Sharing and Analysis Center (FS/ISAC) in 1999 to provide a facility for anonymously gathering information on threats, vulnerabilities, incidents, resolutions, and solutions among industry participants and ultimately to and from government sources. The FS/ISAC is a productive and necessary first step.

There are, however, significant barriers to information sharing and vulnerability assessments. The Freedom of Information Act (FOIA) was designed to provide information to the public on government actions, but some companies are reluctant to share vulnerability information with the government for fear of a subsequent FOIA request. For example, some public utilities are reluctant to conduct vulnerability assessments because their state laws require full disclosure to the public—and such disclosure may undermine consumer confidence, which would vastly complicate efforts to make improvements. Sunshine laws vary widely among the states, complicating the issue even further. Today some corporate counsels advise against voluntarily sharing the details of computer attacks with government agencies because of these concerns.

Members of the financial services sector understand the type of data that needs to be shared with the Federal government for homeland security and critical infrastructure purposes. Information generally covers the health of the financial markets and the assets and infrastructure supporting delivery of the most critical services for homeland security purposes. Specifically, BITS and the FSR believe that information exchanges should involve enhancing security and managing risk (preparedness, response, mitigation, and recovery) of assets and services recognized as nationally significant such as the payments, settlement, and clearance systems. Critical information additionally covers assets that, if attacked, could significantly undermine public trust and confidence. To that end, our members support legislation designed to create a robust environment for the voluntary sharing of information. Such legislation should accomplish several important goals:

> FOIA Coverage: The unique information sharing needs of the financial services community support a limited FOIA exemption. We support a narrowly crafted FOIA exemption statue. Often referred to as a "(b)(3)" FOIA statue, Congress recognizes the need for these exemptions in cases

where the existing FOIA exemptions/exceptions insufficiently protect certain confidential or proprietary data from disclosure or offer insufficient protection for public policy purposes. The pending legislation (S. 1456, Bennett-Kyl, and H.R. 2435, Davis-Moran) takes significant steps toward correcting this situation by protecting the information from disclosure.

Anti-trust law and policy: Businesses also need protection from unnecessary restrictions placed by federal and state antitrust laws on critical information sharing that would inhibit the identification and mitigation of vulnerabilities. The FSR believes that antitrust impediments are significant and should similarly be addressed to facilitate information sharing between infrastructure owners and the Federal government. When companies share information about protecting employees and critical assets, such discussions should not place these businesses at risk of potential antitrust action by federal, state or private parties. The aforementioned legislation includes a limited immunity for antitrust purposes for information shared solely for the purposes of facilitating the protection of critical infrastructures.

Liability: Faced with the prospect of unintended liabilities, we also believe that any assurances that Congress can provide to companies voluntarily collaborating with the government in risk management planning activity—such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information—will be very beneficial. Establishing liability safeguards to encourage the sharing of threat and vulnerability information will add to the robustness of the partnership and the significance of the information shared. The bill also provides limited use protection (not immunity) so that critical infrastructure information disclosed to the government cannot subsequently be used against the person submitting the information. However, we believe that the same information-sharing liability exemption provisions during the Y2K period should apply to this legislation.

Thank you for addressing our views on this important subject. We think that an effective legal and public policy framework will contribute to the success of the institutional, information-sharing, technological, and collaborative strategies necessary to protect our nation's economy.

FOR ADDITIONAL INFORMATION

Catherine A. Allen, CEO
BITS
805 15th Street NW, Suite 600
Washington DC 20005
(202) 289-4322 Phone
(202) 289-0193 Fax

○