AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# H.R. 4246, THE CYBER SECURITY INFORMATION ACT OF 2000: AN EXAMINATION OF ISSUES INVOLVING PUBLIC-PRIVATE PARTNERSHIPS FOR CRITICAL INFRASTRUCTURES

## HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

**H.R. 4246**

TO ENCOURAGE THE SECURE DISCLOSURE AND PROTECTED EXCHANGE OF INFORMATION ABOUT CYBER SECURITY PROBLEMS, SOLUTIONS, TEST PRACTICES AND TEST RESULTS, AND RELATED MATTERS IN CONNECTION WITH CRITICAL INFRASTRUCTURE PROTECTION

JUNE 22, 2000

**Serial No. 106–223**

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

72–361 DTP WASHINGTON : 2001

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

## COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

---

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
LISA SMITH ARAFUNE, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

## SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

### EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
BONNIE HEALD, *Director of Communications*
BRYAN SISK, *Clerk*
MICHELLE ASH, *Minority Counsel*

# CONTENTS


| | Page |
|---|---|
| Hearing held on June 22, 2000 | 1 |
| Text of H.R. | 3 |
| Statement of: | |
| Johnstone, Ambassador L. Craig, senior vice president, International Economic and National Security Affairs, U.S. Chamber of Commerce | 67 |
| Oslund, Jack, chairman, Legislative and Regulatory Working Group of the National Security Telecommunications Advisory Committee | 74 |
| Sobel, David L., general counsel, Electronic Privacy Information Center | 78 |
| Tritak, John, Director, Critical Infrastructure Assurance Office, U.S. Department of Commerce | 57 |
| Willemssen, Joel C., Director, Accounting and Information Management Division, U.S. General Accounting Office | 20 |
| Woolley, Daniel, president and chief operating officer, Global Integrity Corp | 86 |
| Letters, statements, etc., submitted for the record by: | |
| Davis, Hon. Thomas M., a Representative in Congress from the State of Virginia, prepared statement of | 15 |
| Horn, Hon. Stephen, a Representative in Congress from the State of California, Presidential Decision Directive 63 | 42 |
| Johnstone, Ambassador L. Craig, senior vice president, International Economic and National Security Affairs, U.S. Chamber of Commerce, prepared statement of | 69 |
| Oslund, Jack, chairman, Legislative and Regulatory Working Group of the National Security Telecommunications Advisory Committee, prepared statement of | 76 |
| Sobel, David L., general counsel, Electronic Privacy Information Center, prepared statement of | 81 |
| Tritak, John, Director, Critical Infrastructure Assurance Office, U.S. Department of Commerce, prepared statement of | 61 |
| Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of | 11 |
| Willemssen, Joel C., Director, Accounting and Information Management Division, U.S. General Accounting Office: | |
| Information concerning critical infrastructure protection | 113 |
| Prepared statement of | 22 |
| Woolley, Daniel, president and chief operating officer, Global Integrity Corp., prepared statement of | 91 |

# H.R. 4246, THE CYBER SECURITY INFORMATION ACT OF 2000: AN EXAMINATION OF ISSUES INVOLVING PUBLIC-PRIVATE PARTNERSHIPS FOR CRITICAL INFRASTRUCTURES

---

**THURSDAY, JUNE 22, 2000**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Biggert, Davis, and Turner.

Also present: Representative Moran.

Staff present: J. Russell George, staff director and chief counsel; Bonnie Heald, director of communications; Bryan Sisk, clerk; Will Ackerly, Chris Dollar, and Meg Kinnard, interns; Michelle Ash, and Trey Henderson, minority counsels; Ellen Rayner, minority chief clerk; Jean Gosa, minority clerk; Melissa Wojack; and Amy Herrick.

Mr. HORN. The subcommittee will come to order.

Today's hearing is on a subject that is both important and timely. The security threat posed to our Nation's critical infrastructure is made more apparent each day as computer viruses place at risk the free flow of information in the cyber world.

When you consider that our critical infrastructure is composed of the financial services arena, telecommunications system, information technology, transportation, water systems, electric power, gas and oil sectors, among many others, the threat is one that must be taken seriously. These sectors have traditionally operated independently but coordinated with the Government to protect themselves against threats posed by traditional warfare.

However, in today's environment these sectors must learn how to protect themselves against unconventional threats such as terrorist and cyber attacks. They must also recognize the new vulnerabilities caused by technological advances. As we learned when preparing for the year 2000 rollover, many of the Nation's most critical computer systems and networks are highly interconnected. With the many advances in information technology, most of these sectors are linked to one another which increases

their exposure to cyber threats. What affects one system can affect the other systems.

In the 104th Congress we called upon the administration to study the Nation's critical infrastructure vulnerabilities and to identify solutions to address those vulnerabilities. The administration has identified a number of steps that must be taken in order to eliminate the potential for significant damage to our critical infrastructure. Foremost, among these suggestions is the need to ensure proper coordination between the public and private sectors who represent the Nation's infrastructure community.

The goal of H.R. 4246, which we are examining today, is to encourage cooperation in this vitally important effort. Before I call on the primary author of this proposal, because a number of our members have to be in and out of other markups around the Hill, I now yield to Mr. Moran, who is a coauthor of the legislation, for his opening statement on the bill.

[The text of H.R. 4246 follows:]

HR 4246 IH

106th CONGRESS

2d Session

**H. R. 4246**

To encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection.

**IN THE HOUSE OF REPRESENTATIVES**

**April 12, 2000**

Mr. DAVIS of Virginia (for himself, Mr. MORAN of Virginia, Mr. CUNNINGHAM, and Mr. ROGAN) introduced the following bill; which was referred to the Committee on Government Reform, and in addition to the Committee on the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

**A BILL**

To encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection.

*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 `Cyber Security Information Act'.

## SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS- Congress finds the following:

(1)(A) Many information technology computer systems, software programs, and similar facilities are vulnerable to attacks or misuse through the Internet, public or private telecommunications systems, or similar means.

(B) The problem described in subparagraph (A) and resulting failures could incapacitate systems that are essential to the functioning of markets, commerce, consumer products, utilities, government, and safety and defense systems, in the United States and throughout the world.

(C) Protecting, reprogramming, or replacing affected systems before the problem incapacitates essential systems is a matter of national and global interest.

(2) The prompt, candid, and thorough, but secure and protected, disclosure and exchange of information related to the cybersecurity of entities, systems, and infrastructure--

(A) would greatly enhance the ability of public and private entities to improve their own cyber security; and

(B) is therefore a matter of national importance and a vital factor in minimizing any potential cyber security related disruption to the Nation's economic well-being and security.

(3) Concern about the potential for legal liability associated with the disclosure and exchange of cyber security information could unnecessarily impede the secure disclosure and protected exchange of such information.

(4) The capability to securely disclose and engage in the protected exchange of information relating to cyber security, solutions, test practices and test results, without undue concern about inappropriate disclosure of that information, is critical to the ability of public and private entities to address cyber security needs in a timely manner.

(5) The national interest will be served by uniform legal standards in connection with the secure disclosure and protected exchange of cyber security information that will promote appropriate disclosures and exchanges of such information in a timely fashion.

(6) The `National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue', released by the President on January 7, 2000, calls for the Government to assist in seeking changes to applicable laws on `Freedom of Information, liability, and antitrust where appropriate' in order to foster industry-wide centers for information sharing and analysis.

(b) PURPOSES- Based upon the powers contained in article I, section 8, clause 3 of the Constitution of the United States, the purposes of this Act are--

(1) to promote the secure disclosure and protected exchange of information related to cyber security;

(2) to assist private industry and government in effectively and rapidly responding to cyber security problems;

(3) to lessen burdens on interstate commerce by establishing certain uniform legal principles in connection with the secure disclosure and protected exchange of information related to cyber security; and

(4) to protect the legitimate users of cyber networks and systems, and to protect the privacy and confidence of shared information.

## SEC. 3. DEFINITIONS.

In this Act:

(1) ANTITRUST LAWS- The term `antitrust laws'--

(A) has the meaning given to it in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)), except that such term includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent such section 5 applies to unfair methods of competition; and

(B) includes any State law similar to the laws referred to in subparagraph (A).

(2) CRITICAL INFRASTRUCTURE- The term `critical infrastructure' means facilities or services so vital to the nation or its economy that their disruption, incapacity, or destruction

would have a debilitating impact on the defense, security, long-term economic prosperity, or health or safety of the United States.

(3) CYBER SECURITY- The term `cyber security' means the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems, or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United States, or that threatens public health or safety.

(4) CYBER SECURITY INTERNET WEBSITE- The term `cyber security Internet website' means an Internet website or other similar electronically accessible service, clearly designated on the website or service by the person or entity creating or controlling the content of the website or service as an area where cyber security statements are posted or otherwise made accessible to appropriate entities.

(5) CYBER SECURITY STATEMENT-

(A) IN GENERAL- The term `cyber security statement' means any communication or other conveyance of information by a party to another, in any form or medium including by means of a cyber security Internet website--

(i) concerning an assessment, projection, or estimate concerning the cyber security of that entity, its computer systems, its software programs, or similar facilities of its own;

(ii) concerning plans, objectives, or timetables for implementing or verifying the cyber security thereof;

(iii) concerning test plans, test dates, test results, or operational problems or solutions related to the cyber security thereof; or

(iv) reviewing, commenting on, or otherwise directly or indirectly relating to the cyber security thereof.

(B) NOT INCLUDED- For the purposes of any action brought under the securities laws, as that term is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47)), the term `cyber security statement' does not include statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), or disclosures or writing that when made accompanied the solicitation of an offer or sale of securities.

## SEC. 4. SPECIAL DATA GATHERING.

(a) IN GENERAL- Any Federal entity, agency, or authority may expressly designate a request for the voluntary provision of information relating to cyber security, including cyber security statements, as a cyber security data gathering request made pursuant to this section.

(b) SPECIFICS- A cyber security data gathering request made under this section--

(1) shall specify a Federal entity, agency, or authority, or, with its consent, another public or private entity, agency, or authority, to gather responses to the request;

(2) shall be a request from a private entity, agency, or authority to a Federal entity, agency, or authority; or

(3) shall be deemed to have been made and to have specified such a private entity, agency, or authority when the Federal entity, agency, or authority has voluntarily been given cyber security information gathered by that private entity, agency, or authority, including by means of a cyber security Internet website.

(c) PROTECTIONS- Except with the express consent or permission of the provider of information described in paragraph (1), any cyber security statements or other such information provided by a party in response to a special cyber security data gathering request made under this section--

(1) shall be exempt from disclosure under section 552(a) of title 5, United States Code (commonly known as the `Freedom of Information Act'), by all Federal entities, agencies, and authorities;

(2) shall not be disclosed to or by any third party; and

(3) may not be used by any Federal or State entity, agency, or authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law.

(d) EXCEPTIONS-

(1) INFORMATION OBTAINED ELSEWHERE- Nothing in this section shall preclude a Federal entity, agency, or authority, or any third party, from separately obtaining the information submitted in response to a request under this section through the use of independent legal authorities, and using such separately obtained information in any action.

(2) PUBLIC DISCLOSURE- A restriction on use or disclosure of information under this section shall not apply to any information disclosed generally or broadly to the public with the express consent of the party.

## SEC. 5. ANTITRUST EXEMPTION.

(a) EXEMPTION- Except as provided in subsection (b), the antitrust laws shall not apply to conduct engaged in, including making and implementing an agreement, solely for the purpose of and limited to--

(1) facilitating the correction or avoidance of a cyber security related problem; or

(2) communicating or disclosing information to help correct or avoid the effects of a cyber security related problem.

(b) EXCEPTION TO EXEMPTION- Subsection (a) shall not apply with respect to conduct that involves or results in an agreement to boycott any person, to allocate a market, or to fix prices or output.

## SEC. 6. CYBER SECURITY WORKING GROUPS.

(a) IN GENERAL-

(1) WORKING GROUPS- The President may establish and terminate working groups composed of Federal employees who will engage outside organizations in discussions to address cyber security, to share information related to cyber security, and otherwise to serve the purposes of this Act.

(2) LIST OF GROUPS- The President shall maintain and make available to the public a printed and electronic list of such working groups and a point of contact for each, together with an address, telephone number, and electronic mail address for such point of contact.

(3) BALANCE- The President shall seek to achieve a balance of participation and representation among the working groups.

(4) MEETINGS- Each meeting of a working group created under this section shall be announced in advance in accordance with procedures established by the President.

(b) FEDERAL ADVISORY COMMITTEE ACT- The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the working groups established under this section.

(c) PRIVATE RIGHT OF ACTION- This section creates no private right of action to sue for enforcement of any provision of this section.

*END*

Mr. MORAN. Well thank you very much, Chairman Horn, and thank you for your courtesy. I have got another hearing over in Cannon, but that is very nice of you to do that and appreciate your leadership of this committee. Jim Turner is going to be here shortly, the ranking member, and Tom Davis, the other original sponsor of this legislation. Tom, as I think everyone in this room knows, has been a tremendous leader in the area of information technology and particularly cyber security. We both represent northern Virginia's technology community and this is a terribly important issue.

Every day in America thousands of unauthorized attempts are made to intrude into the computer systems that control key Government and industry networks, including defense facilities, power grids, banks, Government agencies, telephone systems, transportation systems. Some of these attempts fail but too many succeed. Some gain systems administrator status, download passwords, implant snippers to copy transactions, or insert what are called trap doors to permit an easy return.

Some attacks are the equivalent of car thief joy-riders committing a felony as a thrill. They are only mischievous. But others are committed for industrial espionage, theft, revenge-seeking vandalism, or extortion. Some may be committed for intelligence collection, reconnaissance, or creation of a future attack capability. The perpetrators range from juveniles to thieves, from organized crime groups to terrorists, potentially hostile militaries and intelligence services.

What has emerged in the last several years is a dramatic increase in the seriousness of this threat. We know of foreign governments creating offensive attack capabilities against America's cyber networks. America is vulnerable to such attacks because it has quickly become dependent upon computer networks for so many essential services. It has become dependent while paying little attention to protecting those networks. Water, electricity, gas, communications, rail, aviation, and almost all our critical functions are directed by computer controls over vast information systems networks.

In 1995, Presidential Decision Directive 39, what we call PDD 39, directed the Attorney General to lead a Government-wide re-examination of the adequacy of the Nation's infrastructure protection. That review prompted the President to establish in 1996 the President's Commission on Critical Infrastructure Protection, a joint Government and private sector effort to study threats to the Nation's critical infrastructure industries, including cyber security threats.

In October 1997 this organization issued a report that identified the need for a strategy of industry cooperation and sharing of information relating to cyber security, including threats, vulnerabilities, and interdependencies, as the quickest and most effective way to achieve much higher levels of infrastructure protection. The Director of the CIA recently testified before Congress that cyber attacks from other countries and rogue terrorist groups represent the most viable option for leveling the playing field, disarming us in an armed crisis against the United States.

The President's National Plan for Information Systems Protection issued 6 months ago and an earlier Presidential directive have

called on Congress to pass legislation that would encourage information sharing to address these cyber security threats to our Nation's privately held critical infrastructure. That is what this legislation is all about.

When Congressman Davis and I attended the Partnership for Critical Infrastructure meeting at the U.S. Chamber of Commerce the one consistent issue raised by the business community was the sharing of sensitive but important security information. Their concern stemmed from the lack of clarity in antitrust laws and concerns related to disclosures the Government would have to make based on Freedom of Information.

This Freedom of Information Act is the real stumbling point. The challenge posed by the threat of potentially wide spread Y2K failures offered a similar set of problems. It was a parallel situation. In response to those problems, a coalition of businesses worked with the bipartisan coalition in Congress and the administration to meet the same need. Industry cooperation and sharing of information related to Y2K, including threats, vulnerabilities, and interdependencies. Again, it was many of the same people that put that legislation together, and as I mentioned, Tom was the original sponsor of that too. A number of us put together a bipartisan approach and it was effective. And after the passage of that Y2K Information Readiness Disclosure Act, the information began to flow much more freely. And that free flow of information was one of the key reasons why Y2K came and went without significant problems.

A similar remedy addressing the cyber security of the Nation's highly integrated critical infrastructure is necessary to best protect Americans from cyber threats and vulnerabilities. This legislation does just that. It is a balanced approach. There is no issue more important to the health of our economy than ensuring that our Nation's critical infrastructure is protected. Government cannot protect the Nation's infrastructure from cyber attacks without the help of the private sector. As a result businesses must take the lead and work together with the Government to share information so that we can ensure that our Nation's critical infrastructure is protected from cyber attacks and vulnerabilities.

So I am most happy to be cosponsoring the legislation along with my colleague and good friend from Virginia, Tom Davis. Coming out of this subcommittee with its record of achievement with Chairman Horn and Ranking Member Turner, I trust this is going to get speedy passage as well. I applaud this committee for holding this hearing and I trust that as a result we are going to be able to provide the framework that will provide industry with the tools necessary for meeting this challenge. It is important legislation. Thank you very much for having the hearing, Mr. Chairman. I appreciate you giving me the opportunity to make that statement. Thank you.

Mr. HORN. Thank you very much to the gentleman from northern Virginia.

And now I yield to the ranking member, Mr. Turner, the gentleman from Texas.

Mr. TURNER. Thank you, Mr. Chairman. This clearly is one of the most challenging issues that we face, the protection of critical infrastructure. In the interest of time, Mr. Chairman, I think I will submit my statement for the record and yield back my time.

Again, I want to thank Mr. Davis and Mr. Moran for their leadership on the issue.

[The prepared statement of Hon. Jim Turner follows:]

**Statement of The Honorable Jim Turner**
**GMIT Hearing: The Cyber Security Information Act of 2000**
**6/22/00**

Thank you, Mr. Chairman. Critical infrastructure, which is defined as those systems which are essential to the operations of the economy and government, are largely owned and operated in this country by the private sector. The federal government has traditionally coordinated the protection of private sector critical infrastructure from threats posed by traditional warfare. Today, many of our critical infrastructure sectors are linked to one another and face increased vulnerability to cyber threats and terrorists attacks. It is essential that these sectors must learn how to protect themselves against such unconventional threats.

Presidential Decision Directive 63 (PDD-63) and the President's National Plan for Information Systems Protection call on the legislative branch to build the necessary framework to encourage information sharing to address cyber security threats to our nation's privately-held critical infrastructure. The President has called for the creation of Information Sharing and Analysis Centers (ISACs) for each critical infrastructure sector that will be headed by the appropriate federal agency or entity, and a member from its private sector counterpart. Many in the private sector have expressed strong support for this model but are also concerned about the unintended consequences that could result from voluntarily sharing information with the government. Specifically, industry is concerned about potential antitrust violations for sharing information with other industry partners.

In response to these concerns, my colleagues, Rep. Davis and Rep. Moran, both of Virginia, have introduced legislation which attempts to give critical infrastructure industries the assurances they need in order to confidentially share information with the federal government. I appreciate their hard work on this issue. As our nation continues to grow more dependent on information technology, I believe that the protection of our critical infrastructure is one of the most important issues we face in Congress.

However, as we move forward on this issue, I think it is imperative that we keep our commitment to a strong Freedom of Information Act. We should be carefully identifying what additional information may need to be exempted and then we should be weighing the benefits to the public interest in knowing the specific information against any likely harm from disclosure. Again, I commend the Chairman for calling this hearing and welcome the witnesses here this morning.

Mr. HORN. I thank the gentleman.

We now call on the author of the bill, Mr. Davis, the gentleman from northern Virginia.

Mr. DAVIS. Thank you, Mr. Chairman. I would like to thank you for holding this hearing today. It is my hope that today's hearing will facilitate the ongoing dialog in addressing cyber security vulnerabilities and the threats facing our critical infrastructures.

Since this dialog began in 1997 with the creation of the President's Commission on Critical Infrastructure Protection, we have recognized that critical infrastructure security cannot be addressed without partnering with the private sector, as we did with Y2K. Over 80 percent of our critical infrastructure is owned and operated by the private sector. Traditional national defense models do not work in this environment. Instead, we have to look to market forces and voluntary participation in partnerships to successfully protect those infrastructures without burdensome regulations which could unintentionally hurt the competitiveness of U.S. markets.

Critical infrastructures are those systems that are essential to the minimum operations of the economy and the Government. Our critical infrastructures comprise the financial services, telecommunications, information technology, transportation, water systems, emergency services, electrical power, gas and oil sectors in private industry, as well as our national defense, law enforcement, and international security sectors within the Government. Traditionally these sectors operated largely independently of one another and coordinated with the Government to protect themselves against threats posed by traditional warfare.

With the many advances in information technology, many of our critical infrastructure sectors are linked to one another and face increased vulnerability to cyber threats. Technology interconnectivity increases the risk that problems affecting one system will affect other connected systems. Computer networks can provide pathways among systems to gain unauthorized access to data and operations from outside locations if they are not fully monitored and protected.

Attacks on critical infrastructure can come in many different forms. They can originate from groups or persons with malicious intent to destroy or damage our safety and our economy, or from individuals who just enjoy the challenge of attacking and infiltrating computer networks. In a cyber security conference held this past Monday, Richard Clark, the National Security Council staff coordinator for security infrastructure protection and counter-terrorism, issued a warning that the United States faces an electronic Pearl Harbor unless Government and industry work together to strengthen the information security systems protecting our Nation's critical infrastructure. Infiltration of our financial services, telecommunications, and electrical power systems would not be any less devastating than attacks on our military and our nuclear systems.

On May 4th, we were reminded once again that love can be painful. As you know, May 4th is the day the "I love you" viruses rocketed around the globe causing an estimated $8 billion in damages. That figure does not account for the countless frustrations experienced by governments and consumers around the world. Addition-

ally, difference in Government and private-sector response to the virus highlight the need for greater partnership and trust. If the Government had more clearly established channels of communication when this virus hit, it might have avoided significant delays in notifying its own agencies of the virus. I was greatly concerned when I read the General Accounting Office's preliminary results of the Federal Government's handling of the "I love you" virus. The Financial Services Information Sharing and Analysis Center, ISAC, had notified their member companies by 3 a.m. about the virus. But the Federal Bureau of Investigation didn't release its first warning until 11 a.m. Additionally, the Department of Health and Human Services reported that on May 4th the "Love bug" rendered that agency incapable of responding to a biological disaster.

Clearly, this is another area that requires a greater commitment to partnership and coordination between the public and private sectors. I would like to say this is a perfect example of the success of private public partnerships that we need to make a greater commitment to facilitating. The Financial Services ISAC is currently the only one of its kind that is clearly doing its job in getting out timely information.

Moreover, recent studies have demonstrated that the incidence of cyber security threats to both the Government and the private sector are only increasing. According to an October 1999 report issued by the GAO, the number of reported computer security incidents handled by Carnegie Mellon's CERT coordination center has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999. According to information currently posted on CERT's Web site, that number totaled 10,000, doubling the 1998 total for computer security incidents. At this time, Mr. Chairman, I would like to request that the information from CERT's Web site be inserted into the hearing record. Additionally, the Computer Security Institute reported an increase in attacks for the 3rd year in row on responses to their annual survey on computer security.

Because the private sector controls the vast majority of our critical infrastructure, I am concerned that employing a private public partnership to monitor the computer networks, analyze data, issue real time alerts, and employ defenses must be the primary component for protecting Americans. But when we asked the private sector to volunteer some information that otherwise would never be known to external entities, information is often proprietary, which could impose many different liabilities and risks were it to become publicly disseminated. Not surprisingly, we find a great reluctance on these companies to cooperate with the Government.

Mr. Moran and I introduced this bill.

Mr. HORN. May I say the material you and the Chair and the ranking member want to put in at this point, without objection, that is approved.

Mr. DAVIS. Thank you, and I will ask unanimous consent to put the total statement in there.

We introduced this bill to give critical infrastructure industries the assurances they needed in order to confidently share information with the Federal Government. And as we learned with the Y2K model, the Government and industry can work in partnership to produce the best outcome for the American people.

I have a fairly lengthy statement that I would like to ask unanimous consent to have it all in the record. But I would just like to add, Mr. Chairman, I want to thank you for holding this hearing today and look forward to working with you. I appreciate our panelists taking time out from their schedules to share their thoughts on this before we mark this bill up in the subcommittee and then move to full committee. We read your comments and will take them into account and hope for a continuing dialog in this. The challenges that face the Government and the private sector on critical infrastructure security remain very important to us. I hope this legislation will go a long way toward resolving these conflicts. Thank you.

[The prepared statement of Hon. Thomas M. Davis follows:]

THOMAS M. DAVIS

COMMITTEE ON COMMERCE

Congress of the United States
House of Representatives
Washington, DC 20515–4611

**Statement of the Honorable Tom Davis**
**Hearing on H.R. 4246, the Cyber Security Information Act**
**and Public-private Partnerships for Critical Infrastructure Protection**
**Subcommittee on Government Management, Information.,and Technology**
**June 22, 2000**

Mr. Chairman, I would like to thank you for holding this hearing today. It is my hope that today's hearing will facilitate the ongoing dialogue on addressing cyber security vulnerabilities and the threats facing our critical infrastructures. Since this dialogue began in 1997 with the creation of the President's Commission on Critical Infrastructure Protection we have recognized that critical infrastructure security cannot be addressed without partnering with the private sector as we did with Y2K. Over eighty percent of our critical infrastructure is owned and operated by the private sector. Traditional national defense models do not work in this environment. Instead, we must look to market forces and voluntary participation in partnerships to successfully protect those infrastructures without burdensome regulations that could unintentionally hurt the competitiveness of U.S. markets.

Critical infrastructures are those systems that are essential to the minimum operations of the economy and government. Our critical infrastructure is comprised of the financial services, telecommunications, information technology, transportation, water systems, emergency services, electric power, gas and oil sectors in private industry as well as our National Defense, and Law Enforcement and International Security sectors within the government. Traditionally, these sectors operated largely independently of one another and coordinated with government to protect themselves against threats posed by traditional warfare. With the many advances in information technology, many of our critical infrastructure sectors are linked to one another and face increased vulnerability to cyber threats. Technology interconnectivity increases the risk that problems affecting one system will also affect other connected systems. Computer networks can provide pathways among systems to gain unauthorized access to data and operations from outside locations if they are not carefully monitored and protected.

Attacks on critical infrastructure can come in many different forms. They can originate from groups or persons with malicious intent to destroy or damage our safety and

our economy ***or*** from individuals who just enjoy the challenge of attacking and infiltrating computer networks. At a cyber security conference held this past Monday, Richard Clarke, the National Security Council's Staff Coordinator for Security, Infrastructure Protection and Counter-terrorism, issued a warning that the United States faces an "electronic Pearl Harbor" unless government and industry work together to strengthen the information security systems protecting our nation's critical infrastructure. Infiltration of our financial services, telecommunications, and electrical power systems would not be any less devastating than attacks on our military and nuclear systems.

On May 4th, we were reminded once again that love can be painful. As you know, May 4th is the day the "I Love You" virus rocketed around the globe causing an estimated $8 billion in damages. That figure does not account for the countless frustrations experienced by governments and consumers around the world. Additionally, the differnece in government and private sector responses to the virus highlight the need for greater partnership and trust. If the government had more clearly established channels of communication when this virus hit, it might have avoided significant delays in notifying its own agencies of the virus. I was greatly concerned when I read the General Accounting Office's preliminary results of the federal government's handling of the "I Love You" virus. The financial services Information Sharing and Analysis Center (ISAC) had notified their member companies by 3 am about the virus, but the Federal Bureau of Investigation did not release its first warning until 11 am. Additionally, the Department of Health and Human Services reported that on May 4th, the Love Bug rendered that agency incapable of responding to a biological disaster. Clearly, this is another area that requires a greater commitment to partnership and coordination between the public and private sectors.

I would also like to say this is a perfect example of the success of private-public partnerships that we need to make a greater commitment to facilitating. The financial services ISAC is currently the only one of its kind, and it is clearly doing the job in getting out timely information.

Moreover, recent studies have demonstrated that the incidence of cyber security threats to both the government and the private sector are only increasing. According to an October 1999 report issued by the General Accounting Office (GAO), the number of reported computer security incidents handled by Carnegie-Mellon University's CERT Coordination Center has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999. According to information currently posted on CERT's website, that number totaled 10,000, doubling the 1998 total for computer security incidents. At this time, Mr. Chairman, I would like to request that the information from CERT's website be inserted intothe hearing record. Additionally, the Computer Security Institute reported an increase in attacks for the third year in a row based on responses to their annual survey on computer security.

Because the private sector controls the vast majority of our critical infrastructures, I

am convinced that employing a private-public partnership to monitor computer networks, analyze data, issue real-time alerts, and employ defenses, must be the primary component of protecting Americans. But when we ask the private sector to voluntary share information that would otherwise never be known to external entitiesinformation that is often proprietary and which could impose many different liabilities and risks were it to become publicly disclosedwe unsurprisingly find a great reluctance to cooperate with government.

I introduced H.R. 4246 to give critical infrastructure industries the assurances they need in order to confidently share information with the federal government. As we learned with the Y2K model, government and industry can work in partnership to produce the best outcome for the American people. The President has called for the creation of Information Sharing and Analysis Centers (ISACs) for each critical infrastructure sector that will be headed by the appropriate federal agency or entity, and a member from its private sector counterpart. For instance, the Department of Treasury is running the first ISAC for the financial services industry in partnership with Citigroup. Many in the private sector have expressed strong support for this model but have also expressed concerns about voluntarily sharing information with the government and the unintended consequences they could face for acting in good faith. Specifically, there has been concern that industry could potentially face antitrust violations for sharing information with other industry partners, have their shared information be subject to the Freedom of Information Act, or face potential liability concerns for information shared in good faith. My bill will address all three of these concerns. The Cyber Security Information Act also respects the privacy rights of consumers and critical infrastructure operators. Consumers and operators will have the confidence they need to know that information will be handled accurately, confidentially, and reliably.

I understand that concern has been expressed about the structure of the limited FOIA exemption contained in H.R. 4246. I am hopeful that today's hearing will begin an honest dialogue on this and other reasonable concerns that will still afford private sector critical infrastructure operators the assurance they need to share information with the government. FOIA is a hallmark of transparency in government and the success of our republic in the twentieth century. It has served as worldwide model for ensuring accountability in government and ensuring that government serves in the public interest. I do not consider granting a FOIA exemption something to be done without public debate. However, the new models posed by the interconnectivity of our critical infrastructures means that government and the private sector must work together to protect our Nation's security. This presents us with many new challenges including facilitating trust between the public and private sector and ensuring good faith efforts by business are not later used against that business.

I understand that the Center for Democracy and Technology has endorsed a (b)4 FOIA exemption for facilitating information sharing. I commend them for coming to the table. I would like to explore other options that bring us closer together. I do not believe a (b)4 exemption gives us enough assurances for information sharing. At this point, Mr.

Chairman, I would like to ask that an article on EFOIA be inserted in the record. From the August 1997 issue of *Government Executive*, "Virtual Records" contains a section entitled, "Trade Secrets" discussing the (b)4 exemption. Specifically, it states, "The FOIA is not supposed to release commercial secrets to the world. Exemption 4 specifically protects from disclosure "trade secrets and commercial or financial information obtained from a person privileged or confidential." But many a veteran salesman in the federal marketplace can recall receiving a competitor's proposal in response to a FOIA request, thanks presumably to careless processing by the agency. In fact, there have been enough such cases that a provision of the fiscal 1997 Defense authorization act prohibits agencies from releasing most contract proposals."

The Cyber Security Information Act of 2000 is closely modeled after the successful Year 2000 Information and Readiness Disclosure Act by providing a limited FOIA exemption, civil litigation protection for shared information, and an antitrust exemption for information shared within an ISAC. These three protections have been previously cited by the Administration as necessary legislative remedies in Version 1.0 of the National Plan and PDD-63. This legislation will enable the ISACs to move forward so that government and industry may enjoy the mutually cooperative partnership called for in PDD-63. This will also allow us to get a timely and accurate assessment of the vulnerabilities of each sector to cyber attacks and allow for the formulation of proposals to eliminate these vulnerabilities without increasing government regulation, or expanding unfunded federal mandates on the private sector.

We will also ensure that ISACs can move forward to accomplish their missions by developing the necessary technical expertise to establish baseline statistics and patterns within the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a repository of valuable information that may be used by the private sector. As technology continues to rapidly improve industry efficiency and operations, so will the risks posed by vulnerabilities and threats to our infrastructure. We must create a framework that will allow our protective measures to adapt and be updated quickly.

It is my hope that Congress and the Administration can move forward in partnership to provide industry and government with the tools for meeting the information sharing challenge. A Congressional Research Service report on the ISAC proposal describes the information sharing model one of the most crucial pieces for success in protecting our critical infrastructure, yet one of the hardest pieces to realize. With the introduction of the Cyber Security Information Act of 2000, we are removing the primary barrier to information sharing between government and industry. Mr. Chairman, I would also like to note that the National Association of Manufacturers (NAM) sent a letter of support for H.R. 4246 to the Subcommittee and I would like to request that a copy of that letter is inserted into the record.

Again Mr. Chairman, I would like to thank you for holding this hearing today and I look forward to working with you on the many challenges facing the government and the private sector on critical infrastructure security.

Mr. HORN. Well I'm sure it will.

I am particularly grateful to the members of the panel that we are about to swear in. You nobly came here despite the very short notice and we are most grateful to you for having your perspective in this area. So let me just explain how this place works. Mr. Willemssen can tell it better than I can. It's good to see you, Joel. We start down the line based on the agenda. We've got your statements, it is automatically in the record when I introduce you. And second, we would like you, if you can, to not read it because we just do not have that kind of time. And so if you want to take 5 minutes, maybe 8 minutes, that is fine, but just summarize it. The staff and everybody else has gone through the written material, even though that was a last minute affair and we thank each of you for that.

We also swear in all witnesses in this committee. So if you would stand and raise your right hands, and if you have anybody that backs you up, also have them do it.

[Witnesses sworn.]

Mr. HORN. The clerk will note that the six witnesses and the two supporters have taken the oath.

We will start with Mr. Willemssen, the Director of Accounting and Information Management Division of the U.S. General Accounting Office, part of the legislative branch of Government. Mr. Willemssen has great experience with this. He has followed us all over the world on the Y2K situation. I am glad to see you in one place, we don't have to run around the country or the world anymore.

So Mr. Willemssen, we look forward to your overview.

**STATEMENT OF JOEL C. WILLEMSSEN, DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE**

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Ranking Member Turner, Congressman Davis. Thank you for inviting us to testify. It is an honor to appear again before you today. As requested, I will briefly summarize our statement.

Overall, the level of concern over cyber security continues to grow. Understanding cyber security risks and how to best address them are major challenges that the Federal Government has recently begun to address. Earlier this year, the White House released version one of its National Plan for Information Systems Protection. The plan encourages the creation of information sharing and analysis centers to facilitate public and private sector information exchange about actual threats and vulnerabilities. Although such partnerships are central to addressing critical infrastructure protection, some in the private sector have expressed concerns about voluntarily sharing information.

H.R. 4246, the proposed Cyber Security Information Act of 2000, was developed to address these concerns and encourage the disclosure and exchange of information about cyber security problems and solutions. In many respects, the bill is modeled after the year 2000 Information and Readiness Disclosure Act, which provided limited exemptions and protections for the private sector to facilitate the sharing of information on Y2K readiness. In short, the bill

creates an additional protected channel for potentially valuable information that the Federal Government would not otherwise have.

Such information sharing proved invaluable in addressing Y2K. The Y2K Readiness Disclosure Act helped pave the way for disclosures on readiness and available fixes and helped the work of the year 2000 Conversion Council's sector-based working groups. H.R. 4246 could have a similar positive affect. However, there are challenges remaining that need to be addressed to make the legislation a success.

First, the Federal Government needs to be sure it collects the right type of information, that it can effectively analyze this information, and that it can appropriately share the results of its analysis. This is a complex and challenging task, especially given how rapidly threats and vulnerabilities can change.

Second, to effectively engage with the private sector, the Federal Government needs to be a model for computer security. Currently it is not. Audits conducted by us and the Inspectors General show that 22 of the largest Federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data to poor controls over software development and changes.

While a number of factors have contributed to weak information security, the fundamental underlying problem is poor security program management. To attain effective security, several key elements are needed, including: (1) a framework of effective access controls and management oversight; (2) periodic independent audits of agency security programs; (3) more prescriptive guidance on the level of protection required; (4) strengthened incident detection and response capabilities; and (5) adequate technical expertise. Especially important is the need for strong centralized leadership. Such leadership has proven essential to addressing other Government-wide management challenges such as Y2K. And we believe it will be similarly critical in tackling the growing security risks to computer systems and critical infrastructures.

That concludes a summary of my statement. Thank you again for the opportunity to testify, and I will be pleased to address any questions.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

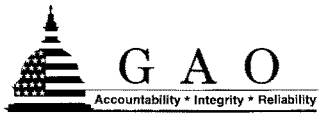
Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
June 22, 2000

# CRITICAL INFRASTRUCTURE PROTECTION

# Comments on the Proposed Cyber Security Information Act of 2000

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division




GAO/T-AIMD-00-229

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the proposed Cyber Security Information Act of 2000 (H.R. 4246), which is intended to remove barriers to information sharing between government and private industry in order to better address threats to the nation's critical infrastructure.

The concern over cyber threats is well placed. While the explosive growth in interconnectivity has contributed immeasurably to the nation's economy and well being, it also presents significant risks to our nation's computer systems and to the critical operations and infrastructures they support, including telecommunications, finance, power distribution, emergency services, law enforcement, national defense, and other government services. Accordingly, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare. Nevertheless, because the federal government does not own all of our nation's critical infrastructures, it is limited in what it can do to protect these assets, and solutions must be tailored sector by sector, through partnerships with sector representatives that address threats, vulnerabilities, and possible response strategies.

Today, I will discuss how H.R. 4246 can enhance critical infrastructure protection and the formidable challenges involved with achieving the goals of the bill. In short, by removing key barriers that are precluding private industry from sharing information about infrastructure threats and vulnerabilities, H.R. 4246 can help build the meaningful

private-public partnerships that are integral to protecting critical infrastructure assets. However, to successfully engage the private sector, the federal government itself must be a model of good information security. Currently, it is not. Significant computer security weaknesses--ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, to nonexistent or weak continuity of service plans--pervade virtually every major agency. And, as illustrated by the recent ILOVEYOU computer virus, mechanisms already in place to facilitate information sharing among federal agencies about impending threats and vulnerabilities have not been working effectively. Moreover, the federal government may not yet have the right tools for identifying, analyzing, coordinating, and disseminating the type of information that H.R. 4246 envisions collecting from the private sector.

**CONCERNS ABOUT RISKS TO OUR CRITICAL INFRASTRUCTURE ARE GROWING**

Before discussing the specifics of H.R. 4246, I would like to provide an overview of the risks of severe disruption facing our nation's critical infrastructure and the steps being taking to address these risks. In particular, the explosive growth in computer interconnectivity over the past 10 years has significantly increased the risk that vulnerabilities exploited within one system will affect other connected systems. Massive computer networks now provide pathways among systems that if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. While the threats or sources of these problems can include natural disasters, such as

earthquakes, and system-induced problems, such as the Year 2000 (Y2K) date conversion problem, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

The resulting damage can vary, depending on the threat. Critical operations can be disrupted or otherwise sabotaged, sensitive data can be read and copied, and data or processes can be tampered with. A significant concern is that terrorists or hostile foreign states could launch computer-based attacks on critical systems, such as those supporting energy distribution, telecommunications, and financial services, to severely damage or disrupt our national defense or other operations, resulting in harm to the public welfare. Understanding these risks to our computer-based infrastructures and determining how best to mitigate them are major information security challenges.

The federal government is beginning to take steps to address those challenges. In 1996, the President's Commission on Critical Infrastructure Protection was established to investigate our nation's vulnerability to both cyber and physical threats. In its October 1997 report, *Critical Foundations: Protecting America's Infrastructures,* the Commission described the potential devastating implications of poor information security from a national perspective.

In May 1998, Presidential Decision Directive 63 (PDD 63) was issued in response to this report and recognized that addressing computer-based risks to our nation's critical

infrastructures required a new approach that involves coordination and cooperation across federal agencies and among public- and private-sector entities and other nations. PDD 63 created several new entities for developing and implementing a strategy for critical infrastructure protection. In addition, it tasked federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors. Since then, a variety of activities have been undertaken, including development and review of individual agency critical infrastructure protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links with the private sector.

In January 2000, the White House released its *National Plan for Information Systems Protection*[1] as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. This plan focuses largely on federal efforts being undertaken to protect the nation's critical cyber-based infrastructures. Subsequent plans are to address a broader range of concerns, including the specific roles industry and state and local governments will play in protecting physical and cyber-based infrastructures from deliberate attacks as well as international aspects of critical infrastructure protection. The end goal of this process is to develop a comprehensive national strategy for critical infrastructure assurance, as envisioned by PDD 63, and to have this plan fully operational in 2003.

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue.* January 7, 2000. The White House.

The plan proposes achieving its twin goals of making the U.S. government a model of information security and developing public-private partnerships to defend our national infrastructure through 10 programs listed in figure 1.

Figure 1: Programs Identified in the National Plan for Information Systems Protection

- Identifying critical infrastructure assets and shared interdependencies
- Detecting attacks and unauthorized intrusions
- Developing intelligence and law enforcement capabilities to protect critical information systems
- Sharing attack warning and information in a timely manner
- Creating capabilities for response, reconstitution, and recovery
- Enhancing research and development
- Training and employing adequate numbers of information security specialists
- Conducting security awareness outreach efforts
- Adopting legislation and appropriations to support infrastructure protections
- Protecting privacy, civil liberties, and proprietary interests

The program involving sharing attack warning and information specifically seeks to bolster information exchange efforts with the private sector. In particular, the program aims to establish a Partnership for Critical Infrastructure Security and a National Infrastructure Assurance Council to increase corporate and government communications about shared threats to critical information systems. It also encourages the creation of Information Sharing and Analysis Centers (ISAC) to facilitate public-private sector information sharing about actual threats and vulnerabilities in individual infrastructure

sectors. Two ISACs are already in operation: (1) the Financial Services ISAC, which exclusively serves the banking, securities, and insurance industries, and (2) the National Coordinating Center for Telecommunications, which is a joint industry/government organization. Several more ISACS are expected to be established by the end of the year.

**H.R. 4246 AND ITS POTENTIAL BENEFITS**

**FOR CRITICAL INFRASTRUCTURE PROTECTION**

Partnerships such as the ISACs are central to addressing critical infrastructure protection. However, some in the private sector have expressed concerns about voluntarily sharing information with the government. For example, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information be subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith.

H.R. 4246 was introduced on April 12, 2000, with the aim of addressing these concerns and encouraging the secure disclosure and exchange of information about cyber security problems and solutions. In many respects, the bill is modeled after the Year 2000 Information and Readiness Disclosure Act, which provided limited exemptions and protections for the private sector in order to facilitate the sharing on information on Y2K readiness. In particular, H.R. 4246:

- protects information being provided by the private sector from disclosure by federal entities under FOIA or disclosure to or by any third party,
- prohibits the use of the information by any federal and state organization or any third party in any civil actions, and
- enables the President to establish and terminate working groups composed of federal employees for the purposes of engaging outside organizations in discuss to address and share information about cyber security.

In essence, the bill seeks to enable the federal government to ask industry questions about events or incidents threatening critical infrastructures, correlate them at a national level in order to build a baseline understanding of infrastructures, and use these baselines to identify anomalies and attacks—something it is not doing now.

Addressing similar concerns proved valuable in addressing the Y2K problem. Although Y2K was a unique and finite challenge, it parallels the critical infrastructure challenge in some important respects. Like critical infrastructure protection, for instance, Y2K spanned the entire spectrum of our national, as well as the global, economy. Moreover, given the scores of interdependencies among private sector companies, state and local governments, and the federal government, a single failure in one system could have repercussions on an array of public and private enterprises. As a result, public/private information sharing was absolutely essential to ensuring compliance in supply chain relationships and reducing the amount of Y2K work.

Early on, Y2K information bottlenecks were widespread in the private sector. According to the President's Council on Year 2000 Conversion,[2] antitrust issues and a natural tendency to compete for advantage made working together on Y2K difficult, if not inconceivable, for many companies. Moreover, the threat of lawsuits had companies worried that they would be held liable for anything they said about the Y2K compliance of products or devices they used or test processes and results for them. Legal considerations also prevented companies from saying anything about their own readiness for date change. Thus, as noted by the council, their business partners, as well as the general public, may have assumed the worst.

According to the council, the Year 2000 Information and Readiness Disclosure Act paved the way for more disclosures about Y2K readiness and experiences with individual products and fixes. Several major telecommunications companies, for example, indicated their willingness to share Y2K information with smaller companies who contacted them. And the leaders of the electric power industry began a series of regional conferences for local distribution companies in which they discussed identified problems and solutions, particularly with embedded chips, as well as testing protocols and contingency planning.

Moreover, the act helped facilitate the work of the more than 25 sector-based working groups established by the council and other outreach activities. For example, the council and federal agencies were able to establish partnerships with several private-sector organizations, such as the North American Electric Reliability Council, to gather

[2] *The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion,* March 29, 2000.

information critical to the nation's Y2K efforts and to address issues such as contingency planning. Concerned about the lack of information in some key industry areas, the council also convened a series of roundtable meetings in the spring and summer of 1999, which helped to shed light on the status of readiness efforts relating to pharmaceuticals, food, hospital supplies, transit, public safety, the Internet, education, and chemicals. The assessment reports resulting from these and other activities substantially increased the nation's understanding of the Y2K readiness of key industries.

Removing barriers to information sharing between government and industry can similarly enhance critical infrastructure protection. Both government and industry are key components of the infrastructure, both are potential targets for cyber threats, and both face significant gaps in effectively dealing with the threats. As such, both must work together to identify threats and vulnerabilities and to develop response strategies. In particular, by combining information concerning the type of incidents and attacks experienced with the information obtained through federal intelligence and law enforcement sources, the government can develop and share more informative warnings and advisories. In turn, companies can develop a better understanding of the threats facing their particular infrastructures and be better prepared to take appropriate actions to protect their sectors.

**CHALLENGES IN BUILDING**

**PUBLIC/PRIVATE PARTNERSHIPS**

By addressing private sector concerns about sharing information, H.R. 4246 could have a positive effect similar to the one the Year 2000 Information and Readiness Disclosure Act had in resolving the Y2K problem. At the same time, there are two formidable challenges to making this legislation a success.

First, while information sharing is important, the government needs to be sure that it is collecting the right type of information, that it can effectively synthesize and analyze it, and that it can appropriately share its analysis. A significant amount of work still needs to be done just in terms of ensuring that the right type of information is collected. For example, what information is required that will enable the government to detect a nationally significant cyber attack? Will information on intrusions, software anomalies, or reports of significant system failures provide an accurate baseline for making these determinations? Today, officials in the intelligence community do not know with real certainty what constitutes a cyber attack. Further, a 1996 Defense Science Board report stressed that understanding the information warfare process and indications of information warfare attacks will likely require an unprecedented effort to collect, consolidate, and synthesize data from a range of owners of infrastructure assets. The ISACs being established to facilitate public-private sector information sharing can assist in meeting this challenge. However, as noted earlier, only two ISACS are in operation

and proposals regarding these centers are presented only in broad terms in the administration's preliminary National Plan for Information Systems Protection.

Once the government is sure that it is asking for the right type of information, it will need effective mechanisms for collecting and analyzing it. Building a common operational picture of critical infrastructures and determining if an attack is underway requires the government to develop capabilities to quickly and accurately correlate information from different infrastructures and reports of security incidents. This is a complex and challenging task in itself. Data on possible threats—ranging from viruses, to hoaxes, to random threats, to news events, and computer intrusions—must be continually collected and analyzed from a wide spectrum of globally distributed sources in addition to sector-based groups. Nevertheless, fusing the right information from the public and private sectors in an operational setting is essential to detecting, warning, and responding to information-based attacks.

The National Infrastructure Protection Center (NIPC), located in the Federal Bureau of Investigation, is charged with this mission, but it is not clear whether NIPC has the right tools and resources needed to successfully coordinate information collection efforts with the private sector and to effectively correlate and analyze information received. We are currently engaged in an effort to review this capability.

In addition to collecting and analyzing data, the federal government needs to be able to effectively share information about infrastructure threats. Again, NIPC is charged with

this responsibility and we are also reviewing its capability with respect to this issue. But, already, results in this area have been mixed. In December 1999, NIPC provided early warnings about a rash of denial-of-service attacks prominently on its website—2 months before the attack arrived in full force--and offered a tool that could be downloaded to scan for the presence of the denial of service code.

However, as we recently testified,[3] NIPC had less success with the ILOVEYOU virus. NIPC first learned of the virus at 5:45 a.m. EDT from an industry source, yet it did not issue an alert about the virus on its own web page until 11 a.m.—hours after many federal agencies were reportedly hit. This notice was a brief advisory; NIPC did not offer advice on dealing with the virus until 10 p.m. that evening. The lack of a more effective early warning clearly affected most federal agencies. Only 7 of 20 we contacted were spared widespread infection, which resulted in slowing some agency operations and requiring the diversion of technical staff toward stemming the virus' spread and cleaning "infected" computers. Moreover, NIPC did not directly warn the financial services ISAC about the impending threat.

The second challenge to realizing the goals of H.R. 4246 is that, to truly engage the private sector, the federal government needs to be a model for computer security. Currently, the federal government is not a model. As emphasized in the National Plan for Information Systems Protection, the federal government

[3] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000) and *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000).

specifically needs to be able to demonstrate that it can protect its own critical assets from cyber attack as well as lead research and development and educational efforts in the field of computer security. However, audits conducted by GAO and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, to nonexistent or weak continuity of service plans.[4]

Importantly, our audits have repeatedly identified serious deficiencies in the most basic controls over access to federal systems. For example, managers often provided overly broad access privileges to very large groups of users, affording far more individuals than necessary the ability to browse, and sometimes modify or delete, sensitive or critical information. In addition, access was often not appropriately authorized or documented; users often shared accounts and passwords or posted passwords in plain view; software access controls were improperly implemented; and user activity was not adequately monitored to deter and identify inappropriate actions.

While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. Agencies have not established the basic

[4] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).

management framework needed to effectively protect their systems. Based on our 1998 study[5] of organizations with superior security programs, this involves managing information security risks through a cycle of risk management activities that include (1) assessing risk and determining protection needs, (2) selecting and implementing cost-effective policies and controls to meet these needs, (3) promoting awareness of policies and controls and of the risks that prompted their adoption, and (4) implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls. Additionally, a strong central focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

I would also like to emphasize that while individual agencies bear primary responsibility for the information security associated with their own operations and assets, there are several areas where governmentwide criteria and requirements also need to be strengthened. Specifically, there is a need for routine periodic independent audits of agency security programs to provide a basis for measuring agency performance and information for strengthened oversight. As we recently testified,[6] a bill has been introduced in the Senate this year—the Proposed Government Information Security Act (S. 1993)—which provides a requirement for such audits. There is also a need for

---

[5] *Executive Guide: Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).
[6] *Information Security: Comments on the Proposed Government Information Security Act of 1999,* (GAO/T-AIMD-00-107, March 2, 2000).

- more prescriptive guidance regarding the level of protection that is appropriate for their systems,
- strengthened central leadership and coordination of information security-related activities across government,
- strengthened incident detection and response capabilities, and
- adequate technical expertise and funding.

For example, central leadership and coordination of information security-related activities across government is lacking. Under current law, responsibility for guidance and oversight of agency information security is divided among a number of agencies, including

- the Office of Management and Budget (OMB), which is responsible for developing information security policies and overseeing agency practices;
- the National Institute of Standards and Technology, which is charged with developing technical standards and providing related guidance for sensitive data; and
- the National Security Agency, which is responsible for setting information security standards for national security agencies.

Other organizations are also becoming involved through the administration's critical infrastructure protection initiative, including NIPC; the Critical

Infrastructure Assurance Office, which is working to foster private-public relationships; and the Federal Computer Incident Response Capability (FedCIRC), which is the central coordination and analysis facility dealing with computer security–related issues affecting the civilian agencies and departments across the federal government. While some coordination is occurring, overall, this has resulted in a proliferation of organizations with overlapping oversight and assistance responsibilities. Absent is a strong voice of leadership and a clear understanding of roles and responsibilities.

As we recently testified,[7] having strong, centralized leadership has been critical to addressing other governmentwide management challenges. For example, vigorous support from officials at the highest levels of government was necessary to prompt attention and action to resolving the Y2K problem. Similarly, forceful, centralized leadership was essential to pressing agencies to invest in and accomplish basic management reforms mandated by the Chief Financial Officers Act. To achieve similar results for critical infrastructure protection, the federal government must have the support of top leaders and more clearly defined roles for those organizations that support governmentwide initiatives.

[7] *Information Security: Comments on the Proposed Government Information Security Act of 1999* (GAO/T-AIMD-00-107, March 2, 2000).

-- -- -- --

In summary, by removing private sector concerns about sharing information on critical infrastructure threats, H.R. 4246 can facilitate private-public partnerships and help spark the dialogue needed to identify threats and vulnerabilities and to develop response strategies. For the concepts in H.R. 4246 to work, however, this legislation needs to be accompanied by aggressive outreach efforts; effective centralized leadership; and good tools for collecting, analyzing, and sharing information. Moreover, the federal government cannot realistically expect to engage private-sector participation without putting its own house in order. Doing so will require concerted efforts by senior executives, program managers, and technical specialists to institute the basic management framework needed to effectively detect, protect against, and recover from critical infrastructure attacks. Moreover, it will require cooperative efforts by executive agencies and by the central management agencies, such as OMB, to address crosscutting issues and to ensure that improvements are realized.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Members of the Subcommittee may have.

CONTACTS AND

ACKNOWLEDGEMENTS

For questions regarding this testimony, please contact Jack L. Brock, Jr. at (202) 512-6240. Individuals making key contributions included Cristina Chaplain, Michael Gilmore, and Paul Nicholas.

(512009)

Mr. HORN. Thank you very much, Mr. Willemssen. That was very helpful.

At this point, I also want to put into the record the President's White Paper, the Clinton administration's Policy on Critical Infrastructure Protection, Presidential Decision Directive 63. Without objection, it will be at this point in the record.

[The information referred to follows:]

# WHITE PAPER

## The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

**May 22, 1998**

# WHITE PAPER
# The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63
# May 22, 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

## I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

## II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;

- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.

- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.

- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

- We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure

Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

4. Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

## Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

| | |
|---|---|
| Commerce | Information and communications |
| Treasury | Banking and finance |
| EPA | Water supply |
| Transportation | Aviation<br>Highways (including trucking and intelligent transportation systems)<br>Mass transit<br>Pipelines<br>Rail<br>Waterborne commerce |
| Justice/FBI | Emergency law enforcement services |
| FEMA | Emergency fire service<br>Continuity of government services |
| HHS | Public health services, including prevention, surveillance, laboratory services and personal health services |
| Energy | Electric power<br>Oil and gas production and storage |

Lead Agencies for Special Functions:

| | |
|---|---|
| Justice/FBI | Law enforcement and internal security |
| CIA | Foreign intelligence |
| State | Foreign affairs |
| Defense | National defense |

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National

Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

**Warning and Information Centers**

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the

National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

## Annex B: Additional Taskings

### Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.

- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.

- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.

- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.

- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.

- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

### Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.

- The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.

- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.

- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

**Internal Federal Government Actions**

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.

- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.

- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.

- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.

- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.

- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based

systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

- GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.

- The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

**Assisting the Private Sector**

In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.

- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.

- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

Mr. DAVIS. Mr. Chairman, I would also like to ask that an article on E-FOIA be inserted in the record from the August 1997 issue of Government Executive Virtual Records. If that could be put in the record as well.

Mr. HORN. Without objection, so ordered.

Our next witness is John Tritak, the Director of the Critical Infrastructure Assurance Office of the U.S. Department of Commerce. We are glad you are here.

**STATEMENT OF JOHN TRITAK, DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, U.S. DEPARTMENT OF COMMERCE**

Mr. TRITAK. Thank you, sir. I want to thank you and the subcommittee for giving me the opportunity to appear here before you today. I, too, will try to be brief and summarize my remarks that are being submitted for the record.

I would like to set the context a little bit, in order to underscore the importance of the discussion that is taking place today. It has been a little over 2 years since President Clinton issued PDD 63, establishing defense of the Nation's critical infrastructure as a national security priority. And in doing so however, he presented a rather unique challenge in which we recognized, perhaps for the first time, that we have a national security challenge that the Federal Government's national security establishment cannot solve alone. With over 90 percent of the Nation's infrastructures being privately owned and operated, the need for industry to take a leadership role in securing the Nation's critical infrastructures is essential.

The goal here is, as much as possible, to find market solutions to deal with the problems of computer security and infrastructure assurance, and then, where market forces fail, the Government would step in, in cooperation with Congress, to address any potential gaps in the interests of national security and defense.

Part of what is essential to industry's leadership is the need for strong collaborative partnering arrangements. One of the things that I find striking is that what we are really talking about here are two different kinds of partnerships. One partnership, and perhaps the more important, is the partnership of industry in which each of the sectors organize themselves to address this problem. Then, of course, there is the partnership between industry and Government to identify areas where collaborative effort makes sense. What is essential to both forms of partnership, however, is the need for information sharing, both to raise awareness, improve understanding, share common experiences, and, as appropriate, to serve as a catalyst for action.

Within industry itself, a lot of progress has been made in establishing effective information sharing arrangements. In the telecommunications area, the National Communications Center under the leadership of the NSTAC, which Dr. Oslund will talk about later, was really one of the first effective information sharing arrangements to deal with national security concerns. More recently, the banking and finance industry established an information sharing and analysis center to share important and sensitive information about threats and vulnerabilities in that industry. The North

American Electric Reliability Council recently established a pilot program with the National Infrastructure Protection Center housed at the FBI, to share certain types of information on threats to the electric power industry as a whole. Both the NERC and the National Petroleum Council are working with the Department of Energy to develop a coherent sector plan for addressing threats and vulnerabilities and to share arrangements. Shortly, the information technology industry, under the leadership of Harris Miller of the Information Technology Association of America, is going to establish an information technology ISAC in response to the computer summit that President Clinton held last February as a result of the denial of service attacks that we saw.

When we talk about industry taking a leadership role, we are starting to see that played out in a lot of different ways. We are also seeing increasingly good working relationships between industry sectors and their Federal lead agency counterparts in the Federal Government. For example, the Commerce Department's National Telecommunications and Information Administration is responsible for working closely with the information technology and telecommunications industry, and of course the National Security Telecommunications Advisory Council [NSTAC] has actually played a very important role in helping to guide that dialog and to provide very useful and affective suggestions on how to go forward.

One of the things that becomes clearer as you go further into this issue is that, because industry is increasingly becoming part of the same digital nervous system, you cannot address critical infrastructure security in a stovepipe fashion. The digital age does not recognize the distinctions between the transportation sector, the electric power industry, and telecommunications. And so there is a growing need within industry to discuss and meet with representatives of the respective sectors to determine where the common issues of concern are and how they might be addressed.

There is also a need, if you are going to maximize the market as a means of raising the bar of security across the country, to bring in other stakeholders which includes the risk management community, the investment community, State and local governments, as well as main line businesses who are actually ultimate consumers of the infrastructure of services that generate the wealth of the Nation. And it was with that in mind, that was the impetus for the creation of the Partnership for Critical Infrastructure Security. It serves as a forum for fostering cross-sector dialog to address areas of common concern and experiences with a view toward taking action as appropriate. It also brings in the other professional communities, including the legal community, privacy community, risk-management and the like so that what you have is really a distillation of the markets that is going to have to be involved in this effort if we are going to actually see the security of the Nation's infrastructures improved.

To date there are over 150 companies participating. Congressman Davis and Congress Moran addressed the first working group meeting, and as Congressman Moran indicated in his remarks, it was a very fruitful discussion. Our next meeting will be held in July in San Francisco in which many of the issues that were identified, including issues regarding FOIA, will be further discussed, as

well as industry will begin to engage the Federal Government on how to participate in the next version of the National Plan, which I think is essential to having a national agenda for a new administration to deal with.

I indicated very early on in my remarks that the core of all this is voluntary information sharing, information that does not have to be provided under existing laws and regulations. Some of that information is sensitive. Concerns that the existing statutory environment in any way chills that sort of information sharing therefore must be taken seriously. It was in addressing these concerns that we had a very successful Y2K period, where you saw an unusual and unprecedented amount of the information sharing between Government and between industry. And since I was located very near the ICC, I was able to witness firsthand the success of that.

The President's Commission on Critical Infrastructure Protection acknowledged the importance of dealing with this issue, "We envision the creation of a trusted environment that would allow the Government and private sector to share sensitive information openly and voluntarily. Success will depend on the ability to protect as well as disseminate needed information. We propose altering several legal provisions that appear to inhibit protection and thus discourage participation." The PCCIP went on to include the Freedom of Information Act, antitrust provisions, and protection from liability among the areas that needed to be analyzed. In addition, as I indicated a moment ago, the organizational meeting of the Partnership for Critical Infrastructure Security included in its action items the removal of disincentives to information sharing.

Therefore, I wholeheartedly applaud the intent as well as the objectives of the Cyber Security Information Act that was proposed by Congressmen Davis and Moran. Based on my own experience with these issues over the past years, I believe sharing information regarding common vulnerabilities, threats, and interdependencies is important to effective security controls across the interconnected and shared risk environment within which both Government and industry operate.

The act would create a new exemption from FOIA to protect industry's submitted critical information vulnerability information. As a general matter, we support maximum Government openness while recognizing that certain information such as that relating to cyber vulnerability should be protected from wide dissemination. As with any exemption from Government openness, we need to study this proposal very carefully and need to strike a balance between the goal of information sharing and Government openness. Similarly, we should be confident that the proposed provisions dealing with antitrust and liability protection are measured to achieve their intended goals and not create unintended results.

As the bill points out, prompt, thorough and secure information sharing is clearly a matter of national importance. I think the ability to develop and share designated cyber security information

would be a useful step toward this important goal. We are looking forward to a full and vigorous national discussion on this important legislation. I wish to thank you for the opportunity to testify here today, Mr. Chairman.

[The prepared statement of Mr. Tritak follows:]

**Hearing before the**
**House Government Reform Committee**

**Subcommittee on Government Management, Information and Technology**

**June 22, 2000**

**Statement of**
**John S. Tritak**
**Director**
**Critical Infrastructure Assurance Office**

Mr. Chairman, I am pleased to appear before you today to talk about the important issue of assuring the effectiveness of the Nation's critical infrastructures. I am the Director of the Critical Infrastructure Assurance Office, or CIAO. The CIAO, which is administratively housed at the Department of Commerce, is the primary staff coordination point for the government's efforts to implement Presidential Decision Directive 63 and to develop the National Plan for Critical Infrastructure Protection.

The CIAO was created by PDD-63 to integrate the various industry sector plans into the National Plan, coordinate analyses of the U.S. Government's own dependencies on critical infrastructures, assist in the development of national education and awareness programs, and coordinate legislative and public affairs. To the extent Federal efforts to protect its own critical infrastructures require strengthening the security of related computer systems, the CIAO works closely with members of the Chief Information Officers Council and other responsible officials who are responsible for the actual development and implementation of appropriate Federal computer security programs.

America has long depended on its critical infrastructures for the delivery of services vital to its defense, prosperity, safety and well being. The need for the owners and operators of these infrastructures to plan against and respond to service disruptions caused by either technical failures or natural disasters, such as hurricanes and earthquakes, has existed for as long as there have been electric power plants, gas and oil pipelines, telecommunications networks, railroads, and banks and financial institutions.

In other words, critical infrastructure assurance is not new. What is new is America's growing dependence on information systems and networks to operate those infrastructures. Inter-dependent computer networks are rapidly becoming an integral part of doing business in the Information Age. Restructuring, including deregulation, is driving companies to apply these new technologies more widely to perform core business functions and operations. It is also requiring participation in open markets. An increasing number of transactions are being conducted over the Internet, virtual private networks, and limited dedicated networks. More and more, our nation's infrastructures are being wired together into an ever-expanding digital nervous system. Going on-line is no longer an option, it is a market imperative.

The benefits of all this have been enormous in terms of competitiveness, efficiency and quality of service. But these benefits do not come without risks. The interplay between complexity and technology increases geometrically the different ways technical system failures can occur. More importantly, cyber tools are readily available to individuals or groups to attack and disrupt our infrastructures, whether for fun, profit, revenge, or political or strategic gain. Recent events show that it doesn't take much to cause costly disruptions to the nation's information infrastructure. Just think what those with the resources and motivation might do. One does not have to be an alarmist, nor believe that a massive cyber-attack capable of crippling the nation's infrastructure is just around the corner, to argue for taking preventative action now.

Two years ago President Clinton issued his Presidential Decision Directive 63, establishing the defense of the nation's critical infrastructures against deliberate attacks, particularly those waged in cyberspace, as a national security priority.

In doing so, he presented us with a rather unique national security challenge, one which the Federal Government's national security establishment cannot solve alone. With over 90% of our critical infrastructures being privately owned and operated, assuring the delivery of services vital to the nation's defense and economy must be accomplished in public-private collaboration, with market rather than regulatory solutions being the preferred path.

This is not always easy or quick and those who want rapid solutions should recognize that the need to get all of the relevant parties together will often take time. But I believe that in the long run it is the best approach that we can take, and progress is being made.

President Clinton has requested increased funding for critical infrastructure protection substantially during the past three years, including a 15% increase for the FY2001 budget proposal to $2.0 billion. *The National Plan for Information Systems Protection* was released earlier this year. The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. A significant portion of the current plan aims at putting the Federal Government's own infrastructures in order.

Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback, including, for example, a more detailed focus on privacy considerations. That is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a Dialogue* -- to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment. We hope to issue the next version of the Plan, or at least its outline, by the end of this year.

Industry leadership is essential to protecting our nation's infrastructures. Many of our efforts in government have been directed at raising awareness among industry leaders of the business case for action. They have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can also help identify problems, good practices in management policies and strategies, convene meetings, promote R&D, and investigate legal and legislative reforms, when appropriate.

A strategy of cooperation and partnership within the private sector, as well as between the private sector and the U.S. Government is the foundation upon which our efforts to secure the nation's infrastructures are based. We are committed to building partnerships with the private sector to protect our computer networks.

The Administration's Partnership for Critical Infrastructure Security is just such a collaborative effort between industry and government. The Partnership serves as a forum in which to draw the individual infrastructure sectors together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness and understanding ~~of~~, ~~and to serve~~, ~~when~~ appropriate, as a catalyst for action among, the owners and operators of critical infrastructures, the risk management and investment

communities, other members of the business community, and state and local Governments.

A brief history illustrates the rapid progress being made by the Partnership. Commerce Secretary Daley, Bureau of Export Administration Under Secretary William A. Reinsch, Gregory Rohde, the Assistant Secretary for Communications and Information, and I met with senior members of over 80 Partnership companies in December 1999 in New York, and again In February in Washington, D.C., with over 220 senior members of more than 120 Partnership companies, to encourage business leaders to adopt information security as an integral business practice. The Partnership agreed to address such important issues as cross-sector vulnerability assessments, information sharing, and R&D requirements.

In early February, Secretary Daley met with the President and 25 senior executives concerned about the recent disruptions to the Internet. His meeting reinforced the need for further cooperation between government and industry to help the private sector develop its action agenda for cyber security.

The incidents of early February are not cause for pushing the panic button, but they are a wake up call for action.

The work of the Partnership is ongoing. In July the Partnership will sponsor a plenary conference in San Francisco to continue the process of organization and to evaluate the progress that has been made to date by its working groups.

The Partnership is still very much a work in progress, but it has made dramatic strides in the months since it began.

The Partnership builds on the excellent work already underway between Federal Lead Agencies (i.e., the Department's of Commerce, Defense, Justice, Treasury, Transportation and Energy) and their industry sector counterparts, including communications, banking and finance, transportation, and energy, to promote information sharing arrangements and develop sector plans to address potential vulnerabilities.

Considerable progress has been made in the area of information sharing.

- The financial services industry was one of the first to create an Information Sharing and Analysis Center (ISAC). The Secretary of the Treasury announced the opening of the banking and financial services information security facility, the FS/ISAC, in October 1999. The center is a joint public-private industry initiative designed to facilitate the sharing of information about cyber-threats to the financial services industry.

- As noted in Dr. Oslund's statement, last year, the National Communications Center, under the leadership of the National Security Telecommunications Advisory Committee (NSTAC), established an information sharing center for the telecommunications industry. In addition, members of the NSTAC have been sharing their 18 years of experience in

information sharing with other infrastructure owners and operators as they begin to develop similar arrangements in their own sectors.

- The North American Electric Reliability Council (NERC) has been actively working with the multi-agency National Infrastructure Protection Center (NIPC) to put in place information sharing arrangements on top of their current processes to report on physical events. They have begun a pilot program where electric utility companies and other power entities transmit cyber incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC warning, alert, or advisory to the electric utility community is warranted. In addition, the NIPC and the FBI continue to play a prominent role in developing *InfraGard*, a national cross-sector information sharing and analysis initiative.

- The Department of Energy has been working with both the National Petroleum Council and NERC to develop industry-wide approaches by sharing information on good practices and lessons learned.

- The information technology industry is responding to President Clinton's call during February's White House Computer Summit for that sector to create information sharing arrangements to better deal with deliberate attacks for that sector. This week, Harris Miller, President of the Information Technology Association of America (ITAA), announced that ITAA, as sector coordinator for the information and communications sector, will organize an information technology ISAC. The ISAC will be created in July, and will have a staff that will share real-time information on cyber threats, risks, and vulnerabilities.

One of the key issues cited in the debate on increased information sharing is the removal of disincentives to such sharing. In 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) stated:

> "We envision the creation of a trusted environment that would allow the government and private sector to share sensitive information openly and voluntarily. Success will depend on the ability to protect as well as disseminate needed information. We propose altering several legal provisions that appear to inhibit protection and thus discourage participation."

The PCCIP went on to include the Freedom of Information Act (FOIA), privacy, anti-trust provisions, and protection from liability among the areas that needed to be analyzed. In addition, at its organizational meeting at the beginning of this year, the Partnership for Critical Infrastructure Security included among its action items the removal of disincentive for information sharing. Therefore, we applaud the intent and objectives of the proposed Cyber-Security Information Act.

Based on my experience with these issues over the past year, I believe that sharing of information regarding common vulnerabilities, threats, and interdependencies is important to effective security controls across the interconnected and shared risk environment within which both the government

and industry operate. As the bill points out, promoting prompt, thorough and secure information sharing is clearly a matter of national importance.

H.R 4246 would create a new exemption from FOIA to protect industry submitted critical infrastructure vulnerability information. As a general matter we support maximum government openness while recognizing that certain information, such as that related to cyber vulnerability and voluntarily submitted by industry, should be protected from wide dissemination. As with any exemption from government openness, we need to study this proposal very carefully. While we applaud the objectives of HR 4246, we need to ensure that we are striking the right balance between the goal of information sharing and government openness. Similarly, we should be confident that any proposed provisions dealing with anti-trust and liability protection are measured to achieve their intended goals and do not create unintended results. As the bill points out, promoting prompt, thorough and secure information sharing is clearly a matter of national importance. I think that the ability to develop and share information on common vulnerabilities and incidents between the government and the owners and operators of our critical infrastructure systems would be a useful step toward this important goal. We are looking forward to a full and vigorous national discussion on this important legislation.

Thank you again for this opportunity to testify. I look forward to your questions.

Mr. HORN. Thank you very much, Mr. Tritak. That is very helpful.

We now turn to Ambassador Craig Johnstone, senior vice president for International Economic and National Security Affairs of the U.S. Chamber of Commerce.

Mr. Ambassador, please proceed.

**STATEMENT OF AMBASSADOR L. CRAIG JOHNSTONE, SENIOR VICE PRESIDENT, INTERNATIONAL ECONOMIC AND NATIONAL SECURITY AFFAIRS, U.S. CHAMBER OF COMMERCE**

Ambassador JOHNSTONE. Well thank you very much, Mr. Chairman, and a particular vote of thanks to Mr. Moran and Mr. Davis for having sponsored this very important legislation. I represent the U.S. Chamber of Commerce, the world's largest business organization with 3 million businesses, associations, and chambers represented around the world, and we strongly endorsed this legislation.

Mr. Chairman, we are all witness to the process of globalization and all of the revolutionary changes that we are seeing as a result of new technologies—information management, biotechnology. It has changed the very nature of economic life in our country and it is full of opportunities, but it also brings with it a great number of risks.

There are a new set of security risks unlike those we have ever witnessed previously in our history. These new security risks do not come in the form of foreign armies marching across borders. They're more sophisticated, they're more insidious, and more pervasive. Their providence is more difficult to determine and the defenses are very difficult to mount. These are the threats to our Nation's critical infrastructure, to our computer systems, to our financial infrastructure, to our power grids, to our water supplies. These threats exploit the tools of modern science to attack weak points in our increasingly complex and increasingly vulnerable economic system.

These are very real threats. If you just look in the narrow sector of the threats to the computer infrastructure, you take the CERT Coordination Center's recent report alluded to by Mr. Davis and just take a look at what has happened recently. Over a 2-day period starting February 7th, some of the leading Internet sites of the country came under denial of service attacks from hackers. The sites included Yahoo, eBay, CNN.com, Amazon.com and e-Trade. Less than a month later 350,000 credit card numbers were stolen from the music retailer CD-universe and posted online in an attempt to extort $100,000 from the company. On May 5th the international "Love bug" virus that we are all familiar with struck at enormous cost to American business. And these attempts were perpetrated by amateurs. Imagine the threat were there to be a concerted effort not just of amateurs, but of people working under Government auspices of some kind, somewhere, from some corner of the Earth. The range of weapons that can be brought to bear on a single company today, they can be brought to bear on a single company or they can be brought to bear to affect the lives of millions of people.

Our country must come up with the strategies that address this problem. It does no good for Government to develop a strategy on its own when 90 plus percent of the critical infrastructure of this country is in hands of the private sector. The kind of strategies we need must be developed between industry and Government within individual industries. We can address our critical infrastructure vulnerabilities but only through cooperation and the free flow of information and ideas.

This legislation moves us a step in that direction by establishing trust between industry and Government. You can expect the amount of valuable information exchange on critical infrastructure threats and vulnerabilities to be directly proportional to the amount of safety provided by H.R. 4246. We faced a very similar problem on the Y2K issue and the 1998 Y2K Information and Readiness Disclosure Act paved the way for much smoother relations between the public and private sectors.

Providing a FOIA exemption and an antitrust waiver is critical for the level of success of industry-wide information sharing and analysis centers [ISACs]. These ISACS share information on the nature of vulnerabilities, attempted attacks or unauthorized intrusions, coordinate R&D issues, examine vulnerabilities and dependencies and develop education and awareness programs. This legislation is critical to those efforts, it is also critical to the success of the Partnership for Critical Infrastructure Security, which performs many of the same functions but this time not within industries but between industries, and between industry and government.

I am pleased to say that the U.S. Chamber of Commerce has actively participated in the formation and development of the Partnership for Critical Infrastructure Security and we are pleased to provide ongoing support in collaboration with the Critical Infrastructure Assurance Office and we commend the office for the leadership that it has given on this issue. It's clear from our experience with Y2K, from the requirements of the National Plan, and from the feedback we have received from our own companies, our member companies that this legislation is important, even critical toward accomplishing the cooperation we must have to advance our security goals.

Again, I would like to commend Mr. Davis and Mr. Moran for their leadership in taking on this issue, and I would like to encourage this committee and House to support the Cyber Security Information Act of 2000. Thank you.

[The prepared statement of Ambassador Johnstone follows:]

**STATEMENT**
**on the**
**Cyber Security Information Act of 2000**
**before the**
**Government Reform Committee**
**Government Management, Information, and Technology Subcommittee**
**by**
**Ambassador L. Craig Johnstone**
**Senior Vice President for International, Economic and National Security Affairs**
**U.S. Chamber of Commerce**
**June 22, 2000**

Mr. Chairman and Members of the Committee, thank you for providing the U.S. Chamber of Commerce this opportunity to testify on this important subject. The U.S. Chamber of Commerce is the world's largest business organization, representing more than 3 million businesses, business associations, and chambers of commerce.

We are all witness to a process of globalization and revolutionary new technologies in communications, information management and bio-technology that have changed the very nature of economic life in this country and the world. These are exciting times – the opportunities flowing from these changes are boundless. But, unfortunately, the opportunities have a dark underside. They come with a new set of challenges, a new set of security risks unlike those we have witnessed previously in our history. These new security risks do not come in the form of foreign armies threatening our borders. They are more sophisticated, more insidious, more pervasive. Their provenance is more difficult to predict and mounting an effective defense is more complex.

These are the threats to our nation's critical infrastructure, to our computer systems, to our financial infrastructure, to our power grids, to our water supplies. These threats exploit the tools of modern science to attack weak points in our increasingly connected, complex and vulnerable economic system. Because these threats are real and on-going, it is vital that we create effective public policy to protect our critical infrastructure. The U.S. Chamber of Commerce believes that H.R. 4246 is an important step forward in this process, and we strongly encourage you to support this legislation.

**The Threat To Business**

Why is this legislation necessary? Carnegie-Mellon's CERT Coordination Center, which monitors network security threats, reports that computer security related incidents tripled from 1998 to 1999 to almost 10,000 incidents last year. This year, there have been several notable attacks. Let me give you a quick run down of how some companies were affected by some of the cyber-attacks we have recently experienced:

Over a two-day period starting February 7, some of the leading Internet sites of the country came under distributed Denial-of-Service attacks from hackers. These included: Yahoo, Buy.com, eBay, CNN.com, Amazon.com, ZDNet, E*Trade, and Datek.

Less than a month later, close to 350,000 credit card numbers were stolen from the music retailer CD Universe and posted online in an attempt to extort $100,000 from the company.

On March 2, SalesGate.com reported that 2000 records were taken from its customer database.

On April 25, AboveNet, the host of web sites such as AOL.com, Quotesmith.com and many others, faced a cyber-attack that slowed or shut down many of its clients.

On May 5, the international "Love Bug" virus, apparently created in the Philippines, swept through the United States infecting millions of computers worldwide including an estimated 65% of U.S. companies.

Last Friday, the "Stages" virus began to circulate in the United States and hundreds of companies have reportedly been affected.

You can see why business is very concerned. The range of weapons at the disposal of Internet hackers can be brought to bear on a single company, or they can be used to cripple thousands. What is needed is recognition that as a country the United States has to develop strategies that address the many different facets of this problem. These range from interdependency vulnerability analysis, to prevention, detection, rapid response, and reconstitution of damaged assets. Establishing a sound and proper legislative and public policy framework is an important aspect.

This legislation takes a step forward in this direction.

The purpose of this legislation is to establish trust between businesses within industries, across industries, and between industry and government. This trust is a necessary pre-condition to cooperation.

Our member companies have been very clear about their position on this issue. Government can not expect most companies to voluntarily report information on Critical Infrastructure Protection when it is not in the best interest of the company. The government can expect the amount of valuable information passed on to agencies about Internet threats and vulnerabilities to be directly proportional to the amount of safety provided by H.R. 4246. No protection, no information, plain and simple.

Adequate protection should remove a major disincentive for companies to voluntarily share valuable information for the good of all in industry and government. What is the range and importance of this information? As EDS CEO Dick Brown said in a public speech on June 19th, "...most importantly... we must share attack, vulnerability, and best practices information about cyber threats among companies and governments."

**Learning from the Y2K Experience**

We faced a very similar problem on the Y2K issue. Business was unwilling to expose itself to potential litigation and freedom of information vulnerabilities that would have compromised trade secrets. But we faced up to this problem.

One of the earliest pieces of Y2K legislation, the 1998 Y2K Information and Readiness Disclosure Act, paved the way for much smoother relations between the public and private sectors, and reassured many businesses. The management challenge posed by the threat of potentially widespread Y2K failures brought together a coalition of all types of businesses and a bipartisan coalition in Congress and the Administration to meet the same need.

Industry cooperation and the voluntary sharing of information relating to Y2K, including threats, vulnerabilities and interdependencies, was seen as the quickest and most effective way to achieve much higher levels of Y2K readiness. Even then, the risk that sensitive information provided to the government (even if actually collected and held by private third parties) would find its way into the hands of competitors or antagonists was a widely recognized problem inhibiting voluntary information sharing.

The result of the legislation was that it led companies to adopt strategies of openness and transparency, and ensured that there were clear lines of communication and clear expectations throughout the Y2K transition process. The results speak for themselves: Private/public sector cooperation was superb and crises were averted. A model was established.

We support a similar remedy for today's difficult management problem — the cyber security of the Nation's highly integrated critical infrastructure, and underscore the legislative intent of this bill.

As Representative Davis has said, "the Cybersecurity Information Act is closely modeled after the successful Year 2000 Information and Readiness Disclosure Act to provide a limited Freedom of Information Act (FOIA) exemption, civil litigation protection for shared information, and an antitrust exemption for information shared within an Information Sharing and Analysis Center (ISAC)."

**Developing and Promoting Voluntary Information Sharing Mechanisms**

This initiative fits in with the government's goals as they have developed over the course of the past 5 years. In 1995, Presidential Decision Directive No. 39 (PDD-39) directed the Attorney General to lead a government-wide re-examination of the adequacy of the Nation's infrastructure protection. That review prompted the President to establish, in 1996, the President's Commission On Critical Infrastructure Protection (PCCIP), a joint government and private-sector effort to study threats to the nation's critical infrastructure industries, including cyber security threats. In October 1997, the PCCIP issued a report that identified the need for a strategy of industry cooperation and the voluntary sharing of information relating to cyber security, including threats,

vulnerabilities and interdependencies, as the quickest and most effective way to achieve much higher levels of infrastructure protection.

Ninety percent of the country's critical infrastructure is in the hands of the private sector. Our utility grids, water supplies, transportation network, financial system, Internet infrastructure and telecommunications are well protected in most cases. Nevertheless, advances in new technology and fragmented international political systems have led to new kinds of adversaries, new causes for concern.

Industry is the primary potential target of our new-age criminals and terrorists. Fortunately, industry is taking the lead in addressing the risks. Companies and industries have responded to this threat. Companies like DSFX and iDefense are building up practices in this field, and established giants like IBM, Microsoft, and others are racing to upgrade their capabilities. Government needs to be a part of this process, working to help identify the risks and find solutions. This legislation will improve the ability for the government and industry to work together.

Unfortunately, the first version of the President's National Plan for Information Systems Protection did not reflect significant private sector input, and therefore contained a number of deficiencies. But our government recognized the error and has taken steps to rectify this oversight. In his message accompanying the National Plan, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism noted the private sector's lack of input, and wrote "the Plan, at this stage, does not lay out in great detail what will be done to secure and defend private sector networks." He went on to say that "we earnestly seek and solicit views about [the National Plan's] improvement. As private sector entities make more decisions and plans to reduce their vulnerabilities and improve their protections, future versions of the Plan will reflect that progress."

The National Plan acknowledged that "companies may wish to discuss possible system vulnerabilities with Government experts, but they are deterred from doing so because of the possibility that information disclosed to the Government could become subject to a request for public disclosure under the Freedom of Information Act (FOIA)."

The FOIA exemption and anti-trust waiver are critical to the success of industry-wide Information Sharing and Analysis Centers (ISACs). These ISACs would voluntarily share information among the corporations on the nature of vulnerabilities, attempted attacks or unauthorized intrusions, coordinate R&D issues, examine vulnerabilities and dependencies and develop employee education and awareness programs. The Partnership for Critical Infrastructure Security performs many of the same functions between industries.

These are industry-organized and led organizations, and they are not subject to FOIA. However, they are hybrid organizations in which government representatives are invited to participate, and because of the frictionless nature of information, government participants should protect information they receive through these means as privileged information. What this legislation seeks to do is protect the mechanism and principle of

voluntary information exchange for the purpose of enhancing our critical infrastructure security.

The U.S. Chamber has worked hard to support the ability of the private sector to participate in the National Plan strategic development process. We believe it is an important undertaking, and that it is appropriate that the private sector should be involved and provide input. We have participated in the formation and development of the Partnership for Critical Infrastructure Security. We hosted the Planning Retreat of the Partnership at the Chamber this past February, and we are pleased to provide ongoing administrative and planning support for it in collaboration with the Critical Infrastructure Assurance Office.

Our office at the Chamber fields inquiries every day from companies concerned about the current situation and asking how they can participate. The industry-specific ISACs and the Partnership can provide companies with useful vehicles to provide their input. But before these organizations can be truly effective, companies need to know that the government has taken every step possible to maximize the benefits of this voluntary information-sharing process, and minimize the negative consequences.

The old world model where government bureaucrats had most of the resources and all of the answers is growing obsolete. It only makes sense that as the government goes through its national strategic planning process that it leverage private sector resources and that it appreciate that the private sector may have a lot to contribute.

This is a strategy born out necessity, but which may yield new advantages. Not only will it pave the way for mechanisms like the ISACs and the Partnership to exchange information voluntarily about critical infrastructure threats, but it may lead to new collaborations that will foster further technical development and security advances.

Given our experience with Y2K, the requirements of the National Plan, and the feedback of our companies, we think this legislation will be an important step toward accomplishing some of this country's most important security goals. I would like to commend Mr. Davis and Mr. Moran for their leadership in taking on this issue, and we look forward to working with the Committee to ensure passage of this important legislation.

Thank you.

Mr. HORN. Thank you, Mr. Ambassador.

We now move to Mr. Jack Oslund, the chairman of the Legislative Regulatory Working Group of the National Security Telecommunications Advisory Committee. Mr. Oslund.

**STATEMENT OF JACK OSLUND, CHAIRMAN, LEGISLATIVE AND REGULATORY WORKING GROUP OF THE NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE**

Mr. OSLUND. Thank you, Mr. Chairman. I would like to open up with an apology. I have laryngitis and I will do the best I can. It may govern the speed with which I work against your clock. Thank you for the opportunity to testify here today regarding the President's NSTAC. As you said, I chair the Legislative and Regulatory Working Group of the Industry Executive Subcommittee. My remarks are based on the work of the NSTAC. They do not necessarily represent the views of my company, nor will they address issues on which the NSTAC principals have not taken a formal position.

NSTAC and its representatives have been involved in industry-Government information sharing for 18 years. We have learned many lessons in our various activities that we are always willing to share as other infrastructures begin their own public private partnership arrangements. If the Chair will allow, I would like to provide supporting materials for the committee's use.

Mr. HORN. We will review them and try to get them into the hearing record as best we can, without objection.

Mr. OSLUND. Thank you, sir. What makes information sharing successful? Participants in NSTAC, the NCC, and the NSIEs have built relationships based on trust that fosters the sharing of information. These relationships are largely dependent on individual relationships and the recognition that through cooperation the security of the Nation's critical telecommunications networks can be strengthened.

The NSTAC has examined information sharing initiatives and observed the following: it is already occurring in a number of forums, it may be affected and in some cases it is being affected by legal barriers, it is mostly voluntary, it is dependent on receiving a benefit when voluntarily shared, it is based on trusted relationships, and it may depend upon the company and the individual participant.

The NSTAC also has focused on the potential regulatory and legal barriers which are being discussed today—FOIA, liability, and antitrust. I will limit my oral testimony to FOIA.

FOIA provides the public with access to records maintained by Government departments and agencies. It also sets forth a number of exemptions that allow withholding specific information from disclosure, including proprietary company information. None of these exemptions specifically addresses critical infrastructure protection information that is shared within the ISAC. Yet PDD 63 calls for long-term voluntary information sharing between industry and Government to achieve protection for the Nation's critical infrastructures.

As evidenced by the voluntary information sharing that took place during the Y2K rollover, companies were prepared to share

information with each other and the Government that otherwise would not have been available without the FOIA exemption granted by the Y2K Act.

With respect to information sharing related to critical infrastructure protection, the threat is not as clear as it was for Y2K. The problem is unbounded. There is no fixed deadline for action and, as stated earlier, there currently is no protection from disclosure of critical infrastructure, protection information voluntarily shared with the Government. We are in a continuing dialog with Mr. Tritak and his staff at CIAO on this matter.

The NCC expanded its function to include serving as a telecommunications ISAC this past March. Most industry participants in the NCC feel that the expansion of its activities to include ISAC functions increases the need for protection of information voluntarily shared with Government. To date, FOIA has not been a significant concern in the NCC, primarily because the NCC does not maintain a data base. However, the NCC ISAC is developing an automated information sharing and analysis system that will store data from events and situations reported by participating organizations. As awareness of the NCC and its activities, particularly as an ISAC increases, FOIA requests for the data base may cause participants to be reluctant to share information. It is critical that sensitive company information shared with the Government be protected from disclosure.

Significantly, in May 2000 the NSTAC recommended that the President support legislation to protect critical infrastructure protection information voluntarily shared with the Government from disclosure under FOIA. NSTAC has not yet discussed the pending legislation. It was introduced too late during the last NSTAC work cycle. It will be reviewed during the work cycle that is just beginning.

In conclusion, the lessons learned from the NSTAC's experiences in information sharing are applicable to all critical infrastructures as they begin their own protection efforts. The road to complete trust between and among industry and Government is a long and bumpy one. Legislation is necessary but not sufficient for information sharing. There are other areas that must evolve in order to achieve the level of information sharing sufficient to accomplish the goal of protecting the Nation's critical infrastructures. Technical, logistical, cultural, and human factors issues need to be addressed. While legislation will not solve all the challenges in information sharing, it goes a long way in providing the protection industry needs as well as demonstrating the Government's commitment to being an active member of the information sharing process.

Thank you for inviting me to speak today. I look forward to any questions that you may have.

[The prepared statement of Mr. Oslund follows:]

**Oral Statement of Dr. Jack Oslund, Chairman, Legislative and Regulatory Working Group of the Industry Executive Subcommittee, the President's National Security Telecommunications Advisory Committee, before the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform, United States House of Representatives, Washington, D.C., June 22, 2000**

Thank you, Mr. Chairman, for the opportunity to testify here today regarding the President's National Security Telecommunications Advisory Committee -- NSTAC. Members of the NSTAC are appointed by the President. These members or Principals are very senior officers of their private sector entity, usually CEOs. I chair the Legislative and Regulatory Working Group of the Industry Executive Subcommittee of the President's NSTAC.

My remarks are based on the work of the NSTAC. They do not necessarily represent the views of my company, nor will they address issues on which the NSTAC Principals have not taken a formal position.

NSTAC and its representatives have been involved in industry/Government information sharing for 18 years. We have learned many lessons in our various activities that we are always willing to share as other infrastructures begin their own public-private partnership efforts. If the Chairman will allow, I would like to submit a written statement for the record that expands on the themes I will discuss, as well as supporting materials for the Committee's use.

NSTAC has spent considerable time on the question: What makes information sharing successful? Participants in the NSTAC, the National Coordinating Center for Telecommunications and the Government and Industry Network Security Information Exchanges, have built relationships based on trust that fosters the sharing of information. These relationships, based on corporate associations, are largely dependent on individual relationships and a recognition that through cooperation, the security of the Nation's critical telecommunications networks can be strengthened.

Since the report of the Presidential Commission on Critical Infrastructure Protection, and, more recently, the release of PDD 63, a primary focus of NSTAC has been on gaining an even better understanding of the information sharing process.

The NSTAC has examined information sharing initiatives and observed that information sharing:

- is already occurring in a number of forums,
- may be affected by legal barriers,
- is mostly voluntary,
- is dependent on receiving a benefit when voluntarily shared,
- is based on trusted relationships -- a requirement for any effective information sharing, and
- may be dependent on the company and individual participant.

The NSTAC also has focused on the potential regulatory and legal barriers—the Freedom of Information Act, liability and antitrust—that were identified by the PCCIP. I will limit my oral testimony to FOIA.

FOIA provides the public with access to records maintained by Government departments and agencies. It also sets forth a number of exemptions that allow withholding specific information from disclosure, including proprietary company information. None of these exemptions specifically addresses critical infrastructure protection information that is shared within the Information Sharing and Analysis Center, or ISAC. Yet, PDD 63 calls for long-term voluntary information sharing between industry and Government to achieve protection of the Nation's critical infrastructures.

As evidenced by the voluntary information sharing that took place during the Y2K rollover, companies were prepared to share information with each other and the Government that otherwise would not have been made available without the FOIA exemption granted by the Y2K Information and Readiness Disclosure Act.

With respect to information sharing related to critical infrastructure protection, as discussed in PDD 63, the threat is not as clear as it was for Y2K. The problem is unbounded. There is no fixed deadline for action. And, as stated earlier, there is currently no protection from disclosure of information voluntarily shared with the Government.

The NCC expanded its function to include serving as a telecommunications ISAC this past March. Most industry participants in the NCC feel that the expansion of its activities to include the ISAC function increases the need for protection of information voluntarily shared with Government. To date, FOIA has not been a significant concern in the NCC, primarily because the NCC does not maintain a database of NCC reports. As a result, participation in the NCC and the flow of information between industry and Government has not been impacted by FOIA. However, the NCC-ISAC is developing an automated information sharing and analysis system that will store data from events and situations reported by participating organizations. As awareness of the NCC and its activities, particularly as an ISAC, increases, FOIA requests for the database may cause participants to be reluctant to share information. It is critical that sensitive company information shared with the Government is protected from disclosure under FOIA.

In May 2000, the NSTAC recommended that the President support legislation similar to the Y2K Information and Readiness Disclosure Act to protect critical infrastructure protection information voluntarily shared with the Government from disclosure under FOIA.

The lessons learned from the NSTAC's experiences in information sharing are applicable to all the critical infrastructures as they begin their own protection efforts. The NSTAC, NCC, and NSIEs can each vouch for the fact that the road to complete trust between and among industry and Government is a long and bumpy one. Legislation is necessary, but not sufficient, for information sharing. There are other areas that must evolve in order to achieve the level of information sharing sufficient to accomplish the goal of protecting the Nation's critical infrastructures—technical, logistical, cultural, and human factors issues also need to be addressed. While legislation will not solve all the challenges in information sharing, it goes a long way in providing the protection industry needs as well as demonstrating the Government's commitment to being an active member of the information sharing process.

Thank you for inviting me to speak today and I look forward to any questions you may have.

Mr. HORN. Well thank you, and we wish you well with your laryngitis. There are more allergies on Capitol Hill than anyplace in the world because there is a tree I am told for every tree in the world.

Mr. OSLUND. Mr. Chairman, the doctor did assure me that I do not have a virus bug.

Mr. HORN. Thank you. Let me explain that when you see Members walking in and out now it is because we have a vote on the floor on the rule and we have 15 minutes to respond. Mr. Davis has gone over there. When he comes back, he will preside and I will go over there. We do not like to miss votes.

We will start with Mr. Sobel now, the general counsel of the Electronic Privacy Information Center. Mr. Sobel.

**STATEMENT OF DAVID L. SOBEL, GENERAL COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER**

Mr. SOBEL. Thank you, Mr. Chairman. I appreciate the opportunity to appear today to discuss the Cyber Security Information Act. The Electronic Privacy Information Center, or EPIC, is a frequent user of the Freedom of Information Act. We obtain Government documents on a wide variety of policy areas and we firmly believe that public disclosure of this information improves Government oversight and accountability and really assists the public in becoming fully informed about the activities of the Government.

I have personally been involved with FOIA issues for almost 20 years representing a wide variety of FOIA requesters. In the early 1980's, I assisted in the publication of a book entitled, "Former Secrets," which documented 500 instances in which material released under FOIA served the public interest. I am sure that if there were to be a revision of that book done today in the year 2000, we could easily come up with thousands of such examples of beneficial uses of the Freedom of Information Act.

EPIC, as a member of the FOIA requester community, has, along with other members of that community, for many years expressed concerns about a number of proposals to enact new broad exemptions to the FOIA's disclosure requirements. Most recently, we have joined with scientific, journalist, library, and civil liberties organizations in questioning the need for a new exemption to cover information dealing with the protection of critical infrastructure protections, such as the exemption that would be created in the bill before the subcommittee. We collectively believe that such an approach is fundamentally inconsistent with the basic objectives of FOIA, which is, as the Supreme Court has noted, "to ensure an informed citizenry."

It is clear that as we enter the new century and become increasingly involved in electronic networking that the Government is going to be more and more involved in the protection of critical infrastructure. It is equally apparent that the Government's activity in this area is going to become a matter of increased public interest and debate.

My organization EPIC has monitored developments in this area since the creation of the President's Commission on Critical Infrastructure Protection. After the commission's report came out, we issued a report entitled, "Critical Infrastructure Protection and the

Endangerment of Civil Liberties," in which we raised some questions about possible impacts of some of the proposals. Now while reasonable observers can disagree over the advantages or disadvantages of the commission's proposal, or the more recent initiatives contained in the administration's National Plan, I think we can all agree that critical infrastructure protection raises some significant public policy issues that deserve full and informed public debate.

In fact, public disclosure of information in this area has already helped to shape the administration's policy in the area. As an example, I would cite to the subcommittee the so-called FIDNET proposal, the Federal Intrusion Detection Network, which, as originally proposed, would have subjected private sector computer networks to a potentially invasive monitoring system administered by the FBI. Following news media accounts of that proposal and the negative public reaction, that proposal was significantly scaled back. We at EPIC have received material under the FOIA dealing with these issues, we have made it public, and we think that is an important part of the process, of public debate on these issues.

I would like to focus specifically on the need for the exemption that is contained in this legislation.

Mr. HORN. Let me just interrupt you at this point.

I am going to recess the hearing to go vote. The time remaining is almost expired. Apparently Mr. Davis could not get back in time. But he will pick it up and then have you pick it up.

So we are going to recess for 5 minutes or until Mr. Davis returns.

[Recess.]

Mr. DAVIS. The subcommittee hearing will reconvene.

Mr. Sobel, do you want to continue your remarks.

Mr. SOBEL. Thank you, Congressman Davis. I was pointing out the valuable information that has already been disclosed under the Freedom of Information Act concerning critical infrastructure protection, and citing the example of the initial FIDNET proposal and the revisions that the administration made to that proposal after publication of the details and incorporating the public concern that that engendered. So I think that is a very good example of the importance of public disclosure and the Freedom of Information Act in this particular area.

What I would really like to discuss and focus on in my remaining time is my belief that the Freedom of Information Act, as currently written and construed by the courts, does in fact provide adequate protection for the information that we are discussing and I would maintain really negates the need for a new exemption to be added to the FOIA regime.

I think in looking at this issue, we do need to keep in mind that 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 that we are discussing are located.

The FOIA exemptions that currently exist, in particular I would like to focus on exemption 4, have been the subject of 25 years of litigation. We have extensive caselaw that we can look to. And I believe that caselaw establishes that existing exemption 4 is adequate. For information to come within scope of exemption 4, it

must be shown that the information is either a trade secret or, most significantly here, information which is commercial or financial, obtained from a person, and privileged or confidential. The latter category of information, that is, commercial information that is privileged or confidential, is directly relevant to the issue that is before the subcommittee.

Commercial information is deemed to be confidential "if disclosure of the information is likely to have either of the following effects," and significantly the one we are concerned with here, "To impair the government's ability to obtain the necessary information in the future." My understanding is that H.R. 4246 seeks to ensure that the Government is able to obtain critical infrastructure protection information from the private sector on a voluntary basis. So that concern clearly comes within exemption 4's so-called "impairment" prong.

In fact, 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. This is the critical mass case that the D.C. Circuit decided back in 1992. In essence, the courts defer to the wishes of the private sector submitter and protect the confidentiality of information that the submitter itself does not routinely make public.

In addition to the protections for private sector submitters that are contained in exemption 4 and the relevant caselaw, agency regulations also seek to ensure that protected data is not improperly disclosed. Under the provisions of Executive Order 12600, which President Reagan issued in 1987, agencies are required to give submitters of information an opportunity to submit objections to proposed disclosures and those objections have to be considered by the agency before a disclosure determination is made. The protections don't end there. If the submitter is still unhappy with an agency determination to disclose the submitted information, the submitter can go to the courts, file what is known as a "reverse FOIA" lawsuit and litigate the confidentiality issue. So there are many procedural safeguards already built into the FOIA regime.

I think to a large extent the concern that we hear from industry is really a misperception of existing law. I think this is something that can become a self-fulfilling prophecy. If the agencies responsible for collecting this information are saying to submitters we cannot protect your information, then obviously the flow of information is going to dry up. So I think it is important to direct the efforts toward education and reassuring the private sector submitters that existing law does in fact adequately protect their confidentiality.

I think the FOIA over the last 25 years has worked very well in making these kinds of balances between the need to know, on the one hand, and protecting against harmful disclosures. I would encourage the subcommittee not to upset that delicate balance that we have already developed over the 25 years of litigation. I thank the committee for considering these issues and will be happy to take any questions.

[The prepared statement of Mr. Sobel follows:]

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

**Before the**
**House Committee on Government Reform**
**Subcommittee on Government Management, Information and Technology**

**Hearing on H.R. 4246, the Cyber Security Information Act**

**June 22, 2000**
**Washington, DC**

Mr. Chairman and Members of the Subcommittee:

Thank you for providing me with the opportunity to appear before the Subcommittee to address H.R. 4246, the Cyber Security Information Act. The Electronic Privacy Information Center (EPIC) makes frequent use of the Freedom of Information Act (FOIA) to obtain information from the government about a wide range of policy issues, including 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 almost 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 book today would 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 many years, voiced concerns about various proposals to create broad, wholesale exemptions from the Act's public disclosure provisions. Most recently, EPIC has joined with other right-to-know advocates, including scientific, journalistic, library and civil liberties organizations, in questioning the need for a new FOIA exemption, such as the one contained in H.R. 4246, for information relating to the protection of 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."[1] To accomplish that end, "[d]isclosure, not secrecy, is the dominant objective of the Act."[2]

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*[3]) 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 advantages or disadvantages of the PCCIP's proposals, or the more recent initiatives contained in the Administration's National Plan for Information Systems Protection, I believe we can all agree that critical infrastructure protection raises significant public policy issues that deserve full and informed public discussion.

Public disclosure of relevant information has already helped to shape the scope of Administration policy on critical infrastructure protection. An initial draft of the National Plan called for the creation of the Federal Intrusion Detection Network (FIDNET) which, as originally proposed, would have subjected private sector computer networks to a potentially invasive monitoring system administered by the Federal Bureau of Investigation. After media accounts of the proposal were published, negative public reaction resulted in a modified FIDNET proposal, one that will be limited to government computer networks and operated by the General Services Administration. Even as modified, the FIDNET initiative raises significant legal issues; last year, EPIC released a government memorandum, obtained under the Freedom of Information Act, which indicated that the Department of Justice was aware that the proposal could violate federal wiretap laws. Other records we obtained under FOIA showed that the government plans to use credit card records and telephone toll records as part of the FIDNET system. It is this experience that leads us to question the wisdom of removing information concerning critical infrastructure protection from public view.

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. H.R. 4246 contemplates an automatic, wholesale exemption from the FOIA for "any cyber security statements or other such information provided by a party in response to a special cyber security data gathering

---

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

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

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

request." Given the breadth of the bill's definitions of "critical infrastructure" and "cyber security," I believe the proposed exemption would 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, the proposed exemption is likely to 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 Subcommittee to consider, which is the need for the proposed critical infrastructure exemption. FOIA caselaw developed over the past 25 years 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.

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.[4] The latter category of information (commercial information that is privileged or confidential) is directly relevant to the issue before the Subcommittee. 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."[5] My understanding is that H.R. 4246 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.[6] In essence, the courts defer to the wishes of the

---

[4] Getman v. NLRB, 450 F.2d 670, 673 (D.C. Cir. 1971), stay denied, 404 U.S. 1204 (1971).

[5] National Parks and Conservation Association v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

[6] 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).

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.[7]

In light of the substantial protections against harmful disclosure provided by FOIA Exemption 4 and the caselaw interpreting it, I believe that any private sector reticence to share important data with the government grows out of a misperception of existing law. Indeed, the myth of inadequate protection for such information could become a self-fulfilling prophecy if these misperceptions are not corrected. Rather than amending current law in an effort to address misperceived deficiencies, federal efforts should be directed toward educating and reassuring the private sector as to the broad confidentiality protections provided by the FOIA. Failure to do so will merely inaugurate a new generation of protracted litigation in an area that has already consumed considerable judicial resources, while creating new and unnecessary barriers to public access.

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. I urge the Subcommittee and the Congress to preserve the public's fundamental right to know.

---

[7] See GTE Sylvania, Inc. v. Consumers Union, 445 U.S. 375 (1980).

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 digital surveillance proposal. 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 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 have received any federal grants and/or contracts during the current fiscal year or either of the two previous fiscal years.

Mr. HORN. Thank you very much for being here. I will have some questions for you later.

Mr. Woolley.

**STATEMENT OF DANIEL WOOLLEY, PRESIDENT AND CHIEF OPERATING OFFICER, GLOBAL INTEGRITY CORP.**

Mr. WOOLLEY. Good morning, Congressman Davis, Chairman Horn, members of the subcommittee. I would like to thank you for requesting my perspective on the important issue of information sharing and the quest for cyber security. My name is Dan Woolley and I am the president and chief operating officer for Global Integrity, a company based in Reston, VA.

Global Integrity is a wholly owned subsidiary of Science Applications International Corp., an information security consulting company, and a resource for many Fortune 100 and Global 100 corporations, including online businesses, banks, brokerage houses, insurance companies, telecommunications, and entertainment companies, and other dot-com industries. In this capacity, we test the overall computer security of our client sites, help them develop secure information architectures, and help them to respond to attacks and incidents. We monitor and report to our clients about the most recent threats and vulnerabilities in cyber space, and help them to cooperate with regulations and law enforcement agencies where required or where appropriate.

Global Integrity is also a recognized leader in information sharing to promote cyber security. We established the very first information sharing and analysis center called for by the Presidential Decision Directive, or PDD 63, and since then have established several additional ISACs that have been demanded by the market. Therefore, I am particularly pleased to offer our views today on H.R. 4246, on the state of cyber security, on information sharing and the public-private partnership, including some of the appropriate roles of Government.

Presidential Decision Directive 63 recognized that the critical infrastructure of the United States is not owned by the Government but rather is in the hands of the private sector. While both the Government and the private sector have significant incentive to protect this infrastructure, the ultimate financial responsibility for protecting it lies squarely at the foot of private sector. Moreover, the Government's interest is in protecting the infrastructure against cyber warfare and the deniable service attacks. The private sector's interest is in protecting its infrastructure not only from these attacks but also from attacks by competitors, preventing insider abuse, enforcing corporate policies, protecting investor interest, as well as providing customers with safe, secure, and private means of conducting electronic commerce. While the goals of the private sector and the Government converge, they are not always identical.

We recognize the precariousness of the concept between public and private partnerships on something so sensitive as cyber security, yet we think it a concept worth pursing, albeit it with caution. Certainly the last thing a private company wants is to have its own cyber vulnerabilities publicly exposed to regulators, customers, investors, or competitors. On the other hand, the Government has a

legitimate right to be concerned about the security of the Nation's critical infrastructure and even the security of the businesses that underpin the Nation's economy.

Yet because the private sector owns the infrastructure, we believe they have a primary responsibility for securing it does and should rest with the private sector—those in the financial services, energy, transportation, agriculture, and communications sectors, as well as those in the thousands of IT-dependent businesses. These are the people who own the infrastructure, are familiar with it, and are responsible for making decisions not only about the security, but also about the things like functionality, interoperability, strategic fit, and, of course, cost.

Yet the Government correctly notes that our critical infrastructures are subject to the intrusion and disruption in cyber security if not taken extremely seriously at the very highest levels both within Government and within the private sector. While the private sector should lead, we believe the Government does have a legitimate role in promoting cyber security. The Government must continue in its efforts to recruit and train cyber security professionals and perhaps make laboratory or forensic facilities available to the private sector.

The Government can lead by example, by securing its own infrastructure and by sharing techniques and lessons learned. Global Integrity supports legislative efforts to encourage and even require Government agencies to batten down their own cyber hatches and serve as a model for the private sector. The Government also can help set security standards and best practices to promote education on subjects like computer security, computer forensics, computer law, computer ethics. Finally, the Government can promote private sector cooperation both within the private sector and with the Government by removing any actual or perceived barriers to such cooperation, and by actively and aggressively advocating for such cooperation. The Government should also consider what rewards may be offered to the private sector to encourage safe and secure practices.

According to the Department of Justice statistics, cyber crime cases have increased 43 percent from 1977 to 1999. Threats to the infrastructure are both real and perceived. A survey of 1,000 Americans conducted on June 8–11 this year by the polling firm of Fabrizio McLaughlin Associates found that 67 percent of respondents feel threatened by, or are concerned about cyber crime, and 62 percent believe not enough is being done to protect the Internet consumers against such crime. Sixty-one percent say they are less likely to do business on the Internet as a result of cyber crime, and 65 percent believe online criminals have less of a chance of being caught than criminals in the real world.

We have identified the following trends in cyber attacks: No. 1, distributed attacks are increasing, and abusers take advantage of jurisdictional and sovereignty distinctions to avoid detection and prosecution. No. 2, attackers are using the known and publicized security holes to compromise systems. This is particularly true with respect to the worm type attacks that continue to take advantage of user's willingness to execute unknown and unverified computer programs. No. 3, most incidents and penetrations seem to be

attacks of opportunity, although sophisticated hackers may target specific companies or information with a combination of electronic attacks and deception through social engineering. No. 4, the release of point and click tools has made the ability to take on systems easy and accessible. For example, a well-known tool called B02K, freely available on the Internet, allows an unsophisticated hacker to take over a victim's computer completely, read all files and even turn on attached cameras and microphones to conduct surreptitious surveillance in the room in which the computer is located. No. 5, the increase of the use and potential use of high-speed, always on DSL and cable connections at home increase the risk to both home and corporate attacks. A home user may suffer as many as 40–100 attempted attacks per month on a home DSL connection, ranging from somewhat benign probes to very sophisticated attacks. The attacks come from diverse locations, including Eastern Europe, China, Korea, and other nations in the Far East. The increased of wireless technologies to transmit business critical or personally sensitive information increases the risk of compromise. New security strategies and implementations must be developed for these technologies.

One of the best ways that Government can promote cyber security in the private sector is by encouraging information sharing, and this of course is one of the central objectives of PDD 63. The Directive's charge to create ISACs, Information Sharing Analysis Centers, where information on threats, incidents, vulnerabilities, with associated recommendations and solutions need to be shared and analyzed. This is a critical step in defending against cyber attacks.

When these attacks do occur, companies are often left in the dark, they cannot tell whether the attack is local, regional, or national. They cannot easily determine whether the attack is directed at them alone, their entire industry, or represents part of a series of random or concerted attacks. To defend against potential future attacks, companies must also know about vulnerabilities in the operating systems, applications, browsers, and thousands of the myriads of pieces of software that make up the overall infrastructure. Finally, they must have access to the raw intelligence about the threats to the infrastructure, increased attacks or activity, and new fraud schemes in order to be prepared.

At Global Integrity, we have spent over $3 million in the last 10 months developing the first ISAC for the financial services industry. Thousands of man-hours were dedicated not only by Global, but by dozens of companies led throughout the world by initiatives for the financial services sector toward perfecting this model. The initial goal was to create a broad based model for the financial services industry—banks, insurance companies, brokerages, and other organizations. This model is now being replicated for many companies and sectors around the world.

The FS/ISAC was formally launched in October 1999 and it was based upon the fears of publicity, fears of inviting additional attacks, fears of confidentiality, and fears of antitrust liability.

In the past, the limitations and the willingness of industry members to share information was critical. Today, nobody wants to be

reported on the front page of the Washington Post that their institution has been a victim of an attack or attempted attack.

The FS/ISAC today provides a means for sharing information and for distributing threat data obtained from Government sources without the fear of attribution or publicity. Nothing contained in the FS/ISAC rules or regulations alters the obligations of banks or financial institutions to report these criminal activities. In other words, the decision whether or not to report an incident lies with the victim of the attack, and not with the repository of the collected information. To protect the confidentiality of the information, each paid member issues a series of anonymous certificates which authenticates them but does not specifically identify the member.

We have also recently established the equivalent of news bureaus to collect, analyze, and disseminate information of both regional and national interest. We are establishing bureaus in Asia, Middle East, Central Europe, and the United Kingdom, as well as South America. These regional bureaus are providing incident threat, vulnerability, resolution data regarding events occurring in their regions back to the Reston analysis center for redistribution to all ISAC members on a worldwide basis. The FS/ISAC as well as other ISACs represent a form of public and private cooperation.

As a result of the operation of the FS/ISAC and its advanced warning stations in Asia and Europe, members of the financial services industries that have chosen to participate received early warning about recent threats. For example, the FS/ISAC notified members not only of the methodologies behind the distributed denial of service attacks which were launched last February, but also about specific information indicating that hackers activity was increasing. Indeed, Global took such threats seriously enough to issue generalized news releases on the possibility of such attacks hours before those attacks actually occurred. As Congressman Davis noted, the FS/ISAC advised members about the Love Bug worm several hours before the Government agencies sent out generalized alerts, and provided detailed technical analysis of how these worms worked in the early notification.

There are certain roles and functions that are the province of Government. One, to set minimum standards for security and interoperability, conducting and supporting fundamental research on new security technologies, promoting awareness of issues relating to information protection, ensuring greater international cooperation between law enforcement, Government agencies, and bringing down the barriers which inhibit cooperation.

Finally, a word about the role of Congress in specific. I believe that Congress should take a cautious approach to passing new legislation. We do think that legislation requiring the Government to get its own cyber house in order would be productive. We also think that limited legislation such as H.R. 4246, which removes barriers to information sharing, is a good idea. Whether these barriers are real or perceived is a question on which lawyers cannot agree. However, we know that in many cases perception is a stronger force than reality, and so removing perceived barriers can

be every bit as important to the broader goal, which is to encourage information sharing of incidents, threats, and vulnerabilities.

I thank you, Mr. Chairman, for the opportunity to present our views, and welcome any questions the committee may have.

[The prepared statement of Mr. Woolley follows:]

TESTIMONY OF DANIEL WOOLLEY

PRESIDENT AND CHIEF OPERATING OFFICER

GLOBAL INTEGRITY CORPORATION

BEFORE THE

HOUSE GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

SUBCOMMITTEE

HEARING ON THE CYBER SECURITY INFORMATION ACT

RAYBURN HOUSE OFFICE BUILDING ROOM 2154

June 22, 2000

10:00 AM

Good morning Chairman Horn, Congressman Turner, Congressman Davis, and members of the Subcommittee. Thank you for requesting my perspective on the important issue of information sharing in the quest for cyber security. My name is Dan Woolley, and I am the President and Chief Operating Officer of Global Integrity Corporation, based in Reston, Virginia. Global Integrity, a wholly-owned subsidiary of Science Applications International Corporation (SAIC), is an information security consulting company and a resource for Fortune 100 companies, including online businesses, banks, brokerage houses, insurance companies, telecommunications and entertainment companies and other "dot com" industries. In this capacity, we test the overall computer security of our clients' sites, help them develop secure information architectures, and help them respond to attacks and incidents. We monitor and report to our clients about the most recent threats and vulnerabilities in cyberspace and help them cooperate with regulators and law enforcement agencies where required or where appropriate.

Global Integrity is also a recognized leader in information sharing to promote cyber security. We established the very first Information Sharing and Analysis Center (ISAC) called for by Presidential Decision Directive, or PDD,63, and since then have established several additional ISACs that have been demanded by the market. Therefore, I am particularly pleased to offer our views today on H.R. 4246, on the state of cyber security, on information sharing, and on public/private partnerships, including some appropriate roles for the government.

**The Role of Government and the Private Sector In Securing Critical Infrastructure**

Presidential Decision Directive 63 recognized that the critical infrastructure of the United States is not owned by the government, but rather is in the hands of the private sector. While both the government and the private sector have a significant incentive to protect this infrastructure, the ultimate financial responsibility for protecting it lies squarely at the foot of the private sector. Moreover, the government's interest is in protecting the infrastructure against cyber warfare and total denial of service attacks. The private sector's interest is in protecting its infrastructure not only from these attacks, but also from attacks by competitors, preventing insider abuse, enforcing corporate policies, protecting investor interests, as well as providing customers with safe, secure

and private means of conducting electronic commerce. While the goals of the private sector and the government converge, they are not always identical.

Take the case of a cyber-attack: A hacker breaks into a corporate system, and surreptitiously removes sensitive corporate information, or obtains access to key corporate systems. The chief interest of the company that is the victim of the attack is stop the attack, secure the information, ensure that the vulnerabilities that led to the attack are secured, and only then to even consider – and likely reject – criminal prosecution. The government's interest – from a law enforcement perspective – might be to see that the perpetrator is identified and publicly prosecuted, even if the perpetrator is a corporate insider. Indeed, the publicity that would result from a prosecution (both publicly exposing the vulnerabilities and the fact that they were exploited) could lead to reputational losses, loss of confidence by customers and investors, and ultimately loss of such customers or investors, which can be from 10 to 100 times the actual financial losses resulting from the attack itself. Thus, Global Integrity's corporate customers seek a method of learning about threats, vulnerabilities, and incidents that affect cyber security, without having to expose their own vulnerabilities to the government, or the world.

We recognize the precariousness of the concept of public/private partnerships on something so sensitive as cyber security, yet we think it's a concept worth pursuing -- albeit with caution. Certainly the last thing a private company wants is to have its cyber-vulnerabilities publicly exposed to regulators, customers, investors, or competitors. On the other hand, the government has a legitimate right to be concerned about the security of the nation's critical infrastructure and even the security of the businesses that underpin the nation's economy. Yet because the private sector owns that infrastructure, we believe the primary responsibility for securing it does and should rest with the private sector -- those in the financial services, energy, transportation, agriculture, and communications sectors, as well as those in the thousands of IT-dependent businesses. These are the people who own the infrastructure, are familiar with it, and are responsible for making decisions not only about security, but also about things like functionality, interoperability, strategic fit, and of course, cost.

While security may be of paramount importance to the government, it is only one factor a corporation must take into account in making resource allocation decision. We do believe, however, that as corporations become more dependent upon the electronic infrastructure, and as demands for integrity and privacy increase, the market will and has demanded greater emphasis on security. The government correctly notes that our critical infrastructures are subject to intrusion and disruption if cyber security if not taken extremely seriously at the very highest levels – both within government and in the private sector.

While the private sector should lead, we believe the government does have a legitimate role in promoting cyber security. The government must continue in its efforts to recruit and train cyber security professionals, and perhaps make laboratory or forensic facilities available to the private sector. The government can lead by example – by securing its own infrastructure and sharing techniques and lessons learned. Global Integrity supports legislative efforts that encourage or even require government agencies to batten down their own cyber-hatches. Besides securing key functions in defense, national security, and the many civilian agencies, the government's cyber security initiative can serve as a model to the private sector. The government also can help set security standards and best practices. The government can promote education in public and private colleges and universities on subjects like computer security, computer forensics, computer law, and computer ethics. Finally, the government can promote private sector cooperation – both within the private sector and with the government – by removing any actual or perceived barriers to such cooperation and by actively and aggressively advocating for such cooperation. The government should also consider what rewards may be offered to the private sector to encourage safe and secure computing practices.

**Threats to the Infrastructure – A Nation At Risk**

According to Department of Justice statistics, cybercrime *cases* have increased 43% from 1977 to 1999. Threats to infrastructure are both real and perceived. A survey of 1,000 Americans conducted on June 8-11, 2000, by the polling firm of Fabrizio McLaughlin & Associates found that 67% of respondents feel threatened by or are concerned about cybercrime and 62% believe that not enough is being done to protect Internet consumers against cybercrime. Sixty-one percent say they are less likely to do business on the Internet as a result of cybercrime, and 65 percent believe online

criminals have less of a chance of being caught than criminals in the real world. Reports and analyses conducted by the Computer Security Institute, the FBI, the Computer Emergency Response Team, SANS, as well as Global Integrity Corporation's data confirm the increase of computer related incidents and cyber attacks. By incorporating and synthesizing all available data from government studies, private industry surveys, research/academic research, information security reports, law enforcement statistics, public data and media reports and, most importantly, the live data, intelligence, and incidents worked by GLOBAL INTEGRITY, we have identified the following trends in cyber attacks:

- Distributed attacks are increasing, and abusers take advantage of jurisdictional and sovereignty distinctions to avoid detection or prosecution.
- Compromising the same vulnerabilities in systems is the predominant method of attack. Attackers are using the known and publicized security holes to compromise systems. This is particularly true with respect to the worm type attacks that continue to take advantage of user's willingness to execute unknown and unverified computer programs, thus affecting security and integrity of corporate or other systems.
- Most incidents and penetrations seem to be attacks of opportunity, although sophisticated hackers may target specific companies or information with a combination of electronic attacks and deception through "social engineering."
- The release of point and click tools (complete programs, scripts and virus recipes) has made the ability to hack very easy and accessible to everyone. The numbers of attacks and door knocking have reflected this increase in accessibility and ability. The attacks can be perpetuated by so called "script kiddies" who can download these tools, or by more sophisticated hackers who can create or modify these tools to be more malicious or more difficult to detect. A well-known tool called BO2K, freely available on the Internet, allows an unsophisticated hacker to take over a victim's computer completely, read all files and even turn on attached cameras and microphones to conduct surreptitious surveillance in the room in which the computer is located.
- The increase of the use and potential use of new high-speed "always on" DSL and cable connections at home increase the risk to both home and corporate users to attacks. A home user may suffer as many as 40-100 attempted attacks a month on a home DSL connection,

ranging from the somewhat benign probe to sophisticated attacks. These attacks come from diverse locations, including Eastern Europe, China, Korea and other nations in the Far East.

- The increased use of wireless technologies to transmit business critical or personally sensitive information increases the risk of compromise. New security strategies and implementations must be developed for these technologies.

**Information Sharing in the Private Sector**

One of the best ways the government can promote cyber security in the private sector is by encouraging information sharing, and this, of course, is one of the essential objectives of PDD- 63. The Directive's charge to create ISACs – Information Sharing and Analysis Centers -- where information on threats, incidents and vulnerabilities are shared and analyzed -- is a critical step in defending against cyber attacks. When attacks occur, companies are often left in the dark. They cannot tell whether the attack is local, regional or national. They cannot easily determine whether the attack is directed to them alone, their entire industry, or represents part of a series of random or concerted attacks. To defend against potential future attacks, companies must also know about vulnerabilities in operating systems, applications, browsers, and the thousands of myriad pieces of software that make up the overall infrastructure. Finally, they must have access to raw intelligence about threats to the infrastructure – increased hacker activity or new fraud schemes -- in order to be prepared.

At Global Integrity we spent approximately $3 million over 10 months developing the first ISAC for the financial services sector. We have dedicated the services of our corporate executives, our technical and legal staff, our sales, marketing and promotion staff to making a successful model consistent with the objectives of PDD 63. Thousands of person hours were dedicated not only at Global but also by the dozens of companies that led the initiative within the financial services sector toward perfecting this model. The initial goal was to create a broad based model for the financial services industry – banks, insurance companies, brokerage houses and other financial agencies. This model is now being replicated for other companies, sectors, and government agencies because it is a business model that has been proven to work. I'd like to spend a few minutes describing the Financial Services ISAC.

**The FS/ISAC Model**

To help promote an overall secure infrastructure, the financial services industry was the first to create a formalized mechanism to share information about computer security threats, vulnerabilities and incidents between and among its members. The Financial Services Information Sharing and Analysis Center – FS/ISAC – was formally launched on October 1, 1999 after a press event hosted by Treasury Secretary Somers and SEC Chairman Levitt. The FS/ISAC's activities are directed by separate Limited Liability Corporation representing the broad spectrum of the industry, and are hosted by Global Integrity at its offices in Reston, Virginia. Membership in the FS/ISAC is limited to domestic companies in the financial services industry. The FS/ISAC permits its members to anonymously share information that could help protect the industry as a whole. Fears of publicity, fears of inviting additional attacks, fears of confidentiality, and fears of anti-trust liabilities have, in the past, limited the willingness of industry members to share information. Nobody wants it to be reported in the front page of "The Washington Post" that a bank or financial institution has been the victim of an attack or an attempted attack.

The FS/ISAC provides a means for sharing information – and for distributing threat information obtained from government sources – without fear of attribution or publicity. Nothing contained in the FS/ISAC rules or regulations alters the obligations of banks or other financial institutions to report criminal activities to regulators or law enforcement agencies. Nothing contained in the ISAC regulations precludes or discourages reporting of incidents, except that information learned exclusively from the information provided in the ISAC database remains confidential unless disclosed by the source of that information. In other words, the decision whether or not to report an incident lies with the victim of the attack, and not with the repository of the collected information. To protect the confidentiality of the information, each paid member is issues a series of anonymous certificate that authenticates but does not specifically identify the member.

Members voluntarily submit incident, threat and vulnerability information through a secure web-based server that routes the data in an encrypted and secured form through a series of anonymizers to further ensure its anonymity. When the information arrives at the Reston analysis center, it is examined for authenticity, and analyzed for relevance and urgency. If the information represents

an immediate threat to members, an urgent alert is transmitted – by e-mail, pager, fax or voice communications to all affected members.

We have also recently established the equivalent of "news bureaus" to collect, analyze and disseminate information of both regional and national interest. We are establishing bureaus in Asia, the Middle East, Central Europe, the United Kingdom and South America. These regional "bureaus" will provide incident, threat, vulnerability, and resolution data regarding events occurring in their regions back to the Reston analysis for redistribution to all ISAC members around the world.

The FS/ISAC represents a form of public-private cooperation that is a model for information-sharing initiatives. The Treasury Department and the SEC support but do not run the FS/ISAC. It is a separate entity with its own governing board made up of representatives of various financial institutions. The government may use the FS/ISAC as a means for disseminating information TO members of the financial services industry, but relies on traditional reporting requirements for obtaining information FROM the industry. It works to facilitate inter-corporate information sharing to help protect one of the critical infrastructures and, as a consequence protect the national security.

As a result of the operation of the FS/ISAC, and its advance warning stations in Asia and Europe, members of the financial services industry that have chosen to participate received early warning about recent threats. For example, the FS/ISAC notified members about not only the methodologies behind the distributed denial of service attacks which were launched last February, but also about specific information indicating that hackers activity was increasing. Indeed, Global Integrity took such threats seriously enough to issue a generalized news release about the possibility of such attacks hours before the attacks actually occurred. Although I wish I could claim some prescience about the DDOS attacks, the timing of the press release to coincide with the initiation of the attacks was mere happenstance. The FS/ISAC advised members about the "love bug" worm approximately 4 hours before government agencies sent generalized alerts, and provided detailed technical analysis of how the worm worked and some early defensive strategies. When the more malicious and destructive "new love" worm presented itself some weeks later, the

FS/ISAC alerts preceded government advisories by 12 hours, giving the industry a crucial early warning about this very destructive polymorphic attack. In this way, members were able to take preventative actions that not only secured them, but also effectively limited the spread of the worm. The most recent incident involved the so-called "stages" worm that infected computers on June 18-19 of this year. The FS/ISAC received and disseminated early advisories about this worm that may have prevented greater spread.

When the FS/ISAC model was designed, it was envisioned as a template for voluntary industry cooperation and information sharing in other industries. This has proven to be the case. In fact, following the distributed denial of service attacks in February, Global Integrity was approached by many companies outside of the financial services sector -- some of which didn't fall into any particular sector at all -- and asked about membership in the ISAC. In response to this demand, we created the Worldwide ISAC -- an ISAC that is open to any company in any country. The basic model developed for the FS/ISAC – that promotes early warning and protects anonymity – has been applied to the WW/ISAC.

In addition, working with the Department of Transportation and the General Services Administration, we plan to establish and roll-out a Federal ISAC. Broad participation and a broad willingness to share even very sensitive information are essential for the success of the ISAC model. In our experience, confidentiality and anonymity are crucial to the success of the ISAC.

A similar vehicle for voluntary cooperation has existed in the telecommunications industry for many years. This entity, known as NSTAC – the National Secure Telecommunications Advisory Commission – that includes in its members SAIC, Global Integrity's parent company, facilitates voluntary information sharing in the telecommunications industry.

**Role of the Government**

There are certain roles and functions that are and can be the province of the government. These include setting minimum standards for security and interoperability, conducting and supporting fundamental research on new security technologies -- particularly in the area of biometrics and smart card technologies -- promoting awareness of issues relating to information protection,

ensuring greater international cooperation between law enforcement and other agencies, and bringing down barriers which inhibit such cooperation.

The government should not take upon itself new powers of regulation or impose new burdens upon those operating on the web. Any such regulations would likely be ineffective, counter productive, and would impose a disproportionate compliance burden on U.S. companies. Rather, the government should seek to remove barriers to effective cooperation and encourage the market to make security a priority. The government must respect the fundamental rights of privacy – including a respect for the right of anonymity where appropriate. For political and social discourse to flourish on the web – in America and abroad -- governments must agree not to unduly burden the privacy rights of the electronic community. The government should not use the legitimate threats to computer systems as a justification for increased monitoring or surveillance of its citizens or others. While much of the traffic on the Internet is "public" in the sense that the IP traffic is transmitted over insecure routers and servers, the government should not create a database of "normal" traffic patterns or surveille otherwise innocent Internet traffic.

**Regulatory and Structural Obstacles to Government Private Cooperation**

The present government regulatory structure with respect to computer security is fractured and disjointed, with no individual agency having responsibility for either protecting infrastructure or sharing information about infrastructure threats. This is true both within the government and vis a vis regulation of the private sector. Infrastructure protection responsibility lies with law enforcement, intelligence, defense, and regulatory agencies, from the Department of Energy to the Federal Trade Commission and Department of Justice. A government wide ISAC, with strong participation and non-repudiation to members, will go a long way toward encouraging security within both the public and private sector. Information sharing is a necessary but not sufficient aspect of overall security. Every governmental body must have a Chief Information Officer, much as each body has an independent Inspector General with the possibility of an agency to coordinate all such CIO's. The private sector must be assured that the governmental interest is in protecting infrastructure -- not in regulating, fining or embarrassing the private sector companies that cooperate. The private sector can provide new technologies, new energy and new vitality to the field of computer security, and with trust and encouragement, can work well with the government.

Finally, a word about the role of the Congress in specific. We believe that Congress should take a cautious approach to passing new legislation. We do think that legislation requiring the government to get its own cyber-house in order would be productive. We also think that limited legislation such as H.R. 4246, which removes barriers to information sharing, is a good idea. Whether these barriers are real are perceived is a question on which lawyers cannot agree. However, we all know that in many cases perception is a stronger force than reality, and so removing perceived barriers can be every bit as important to the broader goal, which is to encourage information sharing of incidents, threats and vulnerabilities.

I thank the Chairman for the opportunity to present my views, and welcome any questions the Committee may have.

Mr. HORN. Thank you.

I now recognize Mr. Davis for questioning for 8 minutes.

Mr. DAVIS. I thank you very much, Mr. Chairman.

Let me start with Mr. Sobel, who is probably the most skeptical about the bill. I guess it is your position that we do not need to change FOIA.

Mr. SOBEL. That is correct.

Mr. DAVIS. The problem is that the companies that we want to release the information and share information do not share that view and do not want to have to go through the litigious process of trying to establish that every time they want to release something. That is the difficulty we have.

We have tried to craft a narrow exemption so that it does not do more than we intend it to do. Is there any limiting language that you would find acceptable under this, or is it your strict position that the FOIA law is the FOIA law and we live with it and it will handle all of our needs?

Mr. SOBEL. Let me back up a minute and talk about your opening premise, which is that there is the perception amongst the private sector submitters that there is not currently adequate protection.

Mr. DAVIS. I am going to argue about the law in a minute, but there is certainly the perception.

Mr. SOBEL. Well, I think that the only way to address that perception is to bring people up to speed on what the law is. It is my considered opinion, as well as the opinion of the FOIA requester community that has been involved in the cases that I am citing and frankly has lost a lot of the cases, that the courts give great deference to private sector information that is held by Government agencies. And we can see no scenario under which information that is submitted to the Government voluntarily and that the private sector submitter wishes to maintain the confidentiality of would be disclosed.

So I would prefer to see the resources of the agencies go into reassuring the submitters and get the Justice Department to come forward and say, yes, it is our view that existing law is adequate, and have the Congressional Research Service look at the issue. I am confident that a legal review of that kind will create the kind of reassurance that I think has been lacking thus far.

Mr. DAVIS. So it is not your view that anytime Government is present that there is a public right to know under FOIA, regardless of how that information is obtained.

Mr. SOBEL. The courts have certainly construed all of the exemptions, from my perspective, very broadly. I think the perception out there amongst the requester community is that we have lost most of the big cases, that there has been great deference to both the agencies that seek to withhold information and the private sector submitters of information that do not want the information disclosed. So I think it is pretty clear if you look at the caselaw and the history of the development of exemption 4 that the courts have really bent over backward to make sure that private companies do in fact feel comfortable in voluntarily sharing information with the Government.

I also want to repeat the point that I made in my testimony, which is that it is not only the caselaw that we need to look at, but there was a lot of concern about this issue in the 1980's during the Reagan administration. President Reagan issued Executive Order 12600 which created procedures within all of the agencies to give submitters rights to object.

Mr. DAVIS. But we have had enough of companies that keep coming back that in 1997 the Defense Authorization Act had to prohibit agencies from releasing most contract proposals because there was a lot of proprietary information in the proposals that was leaking out and being FOIAed. This is a constant problem. If you are a private company, and I come out of the private sector, once you give that information out, I think you want ironclad assurance that that information is not going anywhere else either intentionally or sometimes unintentionally, because then you get your trial lawyers, you have antitrust, you have a whole lot of issues that get raised through that.

I guess my question is, what is wrong with clarifying it here? Do you think this is drawn too broadly? We have tried to draw this as narrowly as we can. If we could narrow it in some other way to give everybody the rightful protections, we would be happy to do that.

Mr. SOBEL. I think I would start from the proposition in this area that if it is not broken, why try to fix it, because in the process you might just be creating some new unintended problems. I point out in my written testimony that I think, given the history of FOIA over the last 25 years, that any new exemption or any new language that is inserted into that regime results in protracted litigation.

I think we have devoted considerable judicial resources over the last 25 years to ironing out the meaning of exemption 4. As I say, I think the outcome of that process has been one that is very protective for the private sector. And one of the concerns would be that we are just going to be tied up in litigation for several years as the meaning of this new exemption gets sorted out. Whereas, we have a body of caselaw that we can look at right now that I believe resolves the issue. I think any time you introduce new language into this regime you invite problems.

Mr. DAVIS. Clearly, if you introduce new language, you have new language that has never been litigated before.

Mr. SOBEL. Correct.

Mr. DAVIS. But I think at this point you draw your line way over where what you have said would be assumed and is clarified even further.

Let me just ask Mr. Tritak and others if they would like to comment. Do you feel you have adequate protections at this point under current law?

Mr. TRITAK. Sir, I actually would like to go back to the initial point that you made or this premise of what has been discussed. The fact is there is a debate and it is a debate that is not between lawyers, on one hand, and non-lawyers, on the other. It is a debate among some in the legal community that there is not sufficient clarity about the protections for information sharing.

Now putting aside for a moment the understandable concern that you do not want to change the law, particularly something like FOIA, lightly, we still have the problem and the debate. I think the only way you resolve that is by having that debate and discussing it not only within the legal community, but also you get your owners and operators of infrastructures, the people who are actually expressing these concerns, and their legal counsel to express what it is they are worried about, what is the kind of information that they are concerned may not be protected and under what circumstance.

But I think the fact that there is a debate is the problem that needs to be resolved. The Government and many people believe that the current protections are sufficient. That's fine. But if you are talking about voluntary information and people are concerned that it is not sufficiently clear and they do not provide the information, then arguably you have a public policy goal that you may not be able to achieve.

Mr. DAVIS. It seems pretty clear to me. This is information the Government would have no right to under ordinary circumstance and therefore the public would have no right to under ordinary circumstances. But because we are trying to work together to stop the cyber security threats to our Nation's security, companies are willing to come forward and share information, but only if they can be absolutely sure that their information that they give is going to be protected. The Government would not have it otherwise.

That is all this legislation says. It clarifies it. Without that, as you say, there is debate in the legal community, there are court decisions all over the lot, and you could get something that does not fit within that exemption that you have discussed, Mr. Sobel. I cannot right here say under what circumstances that could be, but somebody could volunteer some information that may not be proprietary but it could be very dangerous if that information were to get out, it could hurt shares of stocks, it could show some exposures, for example, in your own security of your company in terms of somebody coming in potentially and if that information were to get out it could damage among investors and the like. And you would not want that information out, but for the good of national security you are willing to come forward with that. I am not sure under those circumstances that meets the protections of the trade secret protections.

That is our concern, is that we want to make sure when companies come forward, are working in a cooperative venture to attack this enemy called cyber terrorism that we can work together and that nobody is going to be damaged as a result of that.

Does anyone else on the panel want to address that?

Yes, Ambassador Johnstone.

Ambassador JOHNSTONE. Yes, I would. First of all, I would like to start off by saying that I commend Mr. Sobel for his defense of the Freedom of Information Act. The U.S. Chamber of Commerce also strongly believes in the Freedom of Information Act. We have used it on behalf of American business frequently, and we are a strong supporter of the act. However, beyond that, I think we certainly are in disagreement with respect to exclusion 4. For example, he says that exclusion 4 provides adequate protections and

that if business simply understood, through a public education effort of some sort, they would understand that fact. But the fact of the matter is that as soon as we start getting into exchange of information, there will be attorneys who will stand up and say that exemption 4 does not apply to those situations and there will be a debate.

Mr. Sobel points out that that is subject to a review panel process. So now suddenly we have moved from having the protection of the law into something that will be debated within a review panel. Or, alternatively, that there is litigation always possible. So now we have moved it out of the review panel into potential litigation. So that for a company what you do is you face then a very uncertain prospect that may drag you into litigation, or have the assurance of the law and the clarification that is written into the law.

The point that you made, Mr. Davis, I think is the salient point here. That is to say there is nothing written here that is different than what it is Mr. Sobel says is already in the law but which is disputed. So it is a question of clarification and that clarification is critically important for American business. When a businessman has to sit down and decide whether he or she is going to participate in this process, the fact that that clarification has been written into the law is vitally important and I think is the difference that is going to make the difference between cooperation or non-cooperation on this issue.

Mr. SOBEL. If I could just respond briefly. I do not think that the language that the subcommittee is considering is going to preclude litigation in any way. If the agencies' position upon receiving a request is that it is not covered because of this language, that is going to be litigated. So I think we are talking about litigation one way or another if information is submitted and requested and there is a dispute.

My point is that at least under existing exemption 4 we have a body of caselaw that has been developed over the last 25 years and we are not going to have to wait for a lot of clarification on the meaning of new language. I do not think it is a question of litigation or no litigation. I think it is a question of how protracted is that litigation likely to be.

Mr. WOOLLEY. One key point that I would like to make, if you will, from the voice of experience. Companies involved with the financial services ISAC needed to know for certain that that information they were providing to the FS/ISAC was in fact locked down and would never get out or they would not share it. It was mandatory that was involved.

As a result, we spent a tremendous amount of time developing a significant anonymity system with checks and balances and rewrappers that could prove that the information that came in was completely anonymous. That was the only way that the financial services industry would participate. And now we have gotten very, very high participation from that industry and it is that anonymity that has now spawned the international ISAC and the worldwide ISAC that are now providing tremendous inputs.

So I think that the issue needs to be there. If you do not have the anonymity, if you do not have the lock down, American corpora-

tions will not participate. They are too spooked about being dragged into any sort of litigation or disclosure that would be very detrimental to their organizations.

Mr. HORN. Yes, and this will be the last response to it. Go ahead, Mr. Oslund.

Mr. OSLUND. Thank you, Mr. Chairman. In the NCC information sharing process, there is no anonymity when the participants share the information. It is a process that has been going on for a number of years and that is why we stress the trust relationships. Relationships have been developed so companies can share information directly. When we are talking about real time operations, and that is what information sharing for CIP is, you cannot share information under uncertainty. There has to be certainty that you can move this information forward and it will not be challenged.

NSTAC felt FOIA legislation was needed for Y2K. And the conclusions are the same for CIP. The background materials we have provided to the committee, demonstrate these conclusions were reached after a lot of deliberation. Thank you.

Mr. HORN. Thank you.

I now yield 10 minutes to the ranking minority member, Mr. Turner, the gentleman from Texas.

Mr. TURNER. Mr. Sobel, you shared your concern a minute ago that the language in the proposed legislation would not preclude litigation. In fact, your opinion was that it might foment additional litigation. Going beyond that concern, could you please articulate any other concerns that you have about this exemption from liability. Is it your concern that it could be misused, that it could be used as a shield by corporation that might be willing to disclose and therefore they would then be able to hide behind the shield of liability? I assume there is further concern other than the fact that you just think it will result in additional litigation.

Mr. SOBEL. Well, I think from the perspective of the FOIA requester community there is always a concern about Congress stepping into the process of amending a statute that has worked very well for a long time. And there is a general apprehension about creating these piecemeal exemptions. The FOIA, as Congress amended it in 1974, contains nine very specific exemptions that have been construed by the courts and in our opinion really cover all of the harms that we are talking about here.

I should note also it is not just exemption 4. There are situations where exemption 1 for classified information would come into play if we are dealing with defense contractors, for instance. Exemption 7's law enforcement protections would come into play, for instance, if a company is acting in the role as a confidential source. In the context of a hacking investigation, for instance, exemption 7's law enforcement protections would come into play. So the point is that we have a very well-developed FOIA scheme right now and there is a general apprehension to adding on piecemeal exemptions.

Now with particular regard to this area, critical infrastructure protection, I think the concern is that we would be muddying the waters. That you introduce a degree of uncertainty into the FOIA requesting process and the result is likely to be that a new barrier is going to be erected to the disclosure of information that should

properly be disclosed that the subcommittee is not seeking to protect the disclosure of.

So I think it is really a question of just muddying what is today some very settled water in this area and creating yet another excuse for not making information public.

Mr. TURNER. Maybe I need you to pose a hypothetical for me to help me understand your concern. Because the first impression I have when you talk about trying to view this from the point of view of the requester community is that, as I understand it, we are talking about information that the Government does not have and Freedom of Information is always, as I understand it, directed toward information the Government has.

So we are talking about information that were it not voluntarily shared by a corporate entity, the Government would not have it anyway. So from a point of view of the requester community that is interested in preserving access to Government information, it seems to be fairly easy in my mind to say that the requester's concern really should not reach information that the Government really would never have anyway were it not for the voluntary relinquishment of it by private entity.

Mr. SOBEL. I think you have to start from the proposition that once the Government receives information, whether it is under mandatory requirements or provided voluntarily, that information starts to form the basis of what a Government agency is doing and it can in certain instances become an important indication of the operations of that agency. Certainly, for instance, the Food and Drug Administration obtains a lot of information from private companies and in order for the public to really assess what the FDA is doing, you necessarily are going to need some access to that private sector information that has been provided to the agency.

Now on the question of whether or not what we are talking about today is something new, the idea of voluntary submission of information to Government agencies, that is not new. In fact, that is the reason why the cases that I have cited in my testimony have arisen. The courts have specifically dealt with the question under exemption 4 of what should the standards be, what should the rules be when a company voluntarily submits information to an agency.

So I think it is important to recognize that we are not writing on a clean slate here. There have been many instances in the past where agencies have received information voluntarily from private sector submitters, that information has been sought under FOIA, and those are the cases that have developed the caselaw that I am talking about which deals directly with the issue of voluntarily submitted information.

In terms of the importance of this information, to sort of remove this from the theoretical realm, for instance, a local community in which a power plant or a nuclear plant or a water facility is located I think legitimately has some interest in knowing if there are vulnerabilities and safety problems in that facility that might form the basis of a so-called cyber security statement. I think we are going to need some mechanism for sorting that out. There are some very legitimate public interest reasons for making some of this information available.

But again I come back to the way the courts have dealt with these issues. And they have been very protective of the private sector submitters. I believe that the courts have gone too far in this area. I want my position to be clear. I think a lot of the information we are talking about probably should be and could be made public without harm to the private submitter. But the courts have disagreed. But I think there is a lot of important health and safety information that can get caught up in this process.

Mr. TURNER. Thank you.

Mr. HORN. I thank the gentleman. You have 2 minutes remaining. If Mr. Moran would like to get in the 2-minutes here, and then we will yield to Mrs. Biggert for 10.

Mr. MORAN. Thank you, Mr. Horn. I have got to go back to another hearing, so I will leave after my 2 minutes. I appreciate the courtesy. Thank you.

As I mentioned in my opening statement, the reason why Mr. Davis and I returned from the Chamber of Commerce meeting and came up with this legislation is because there was such a widespread view that companies simply could not cooperate to the extent that was necessary and that was requested by the Federal Government and that I think they knew was in their long-term best interest because of their concern about FOIA.

And so we have a situation here where regardless of what your point of view might be, Mr. Sobel, perception is reality. If the general counsels of these firms feel that FOIA is a very serious threat to the privacy of this information and to the viability of their corporation, they are simply not going to cooperate in the way that they know is in the national security interest.

I do not see why it is a problem even if we restate what is existing law. You are suggesting that it may complicate things. And I am only picking on you because you are the only one that has come up with what seems to be such an unreasonable point of view, Mr. Sobel. [Laughter.]

I mean I would not do it if you did not deserve it. I am kidding there. We need somebody to be the devil's advocate here on the panel, and I appreciate you playing that role.

Mr. SOBEL. Glad to do that.

Mr. HORN. And I might add unanimous consent for the participation of our eloquent Irishman today. And hearing no objection, you are free to participate. [Laughter.]

Mr. MORAN. Thank you very much, Mr. Chairman, I appreciate that very much.

Clearly, we do not have the level of participation, the initiative being taken by corporations who have very valuable information to share. And this is the reason why they do not feel that they can. It is not that they do not want to cooperate.

And so even if we are restating legislation clarifying that legislation, as Mr. Davis has suggested, it would seem to be meeting a very important need. And it took what, three decades or something to clarify the meaning of FOIA, three decades of litigation to make it clear what FOIA meant. We cannot afford to go through such an extended process of litigation to clarify the extent of sharing with regard to cyber attacks and cyber vulnerabilities. So it would seem that even if a lawyer might be able to make an argument that you

could share that information, they nevertheless would be subjecting themselves to litigation, and that is what we do not want.

So we want to facilitate the process. We have got very important national security interests at stake here. Every day the sophistication of mischievous and malicious hackers is increased our vulnerabilities increase. As we have stated and as I know you are very much aware of, our entire economic and security infrastructure is at stake. We heard one story about some intelligence officials being given enough money to buy personal computers, two or three dozen of them, and they were told to pretend they were from North Korea and see if they could invade our security infrastructure. And sure enough, within a relatively short period of time they had access to enough computer systems that they could have shut down our power grid and invaded the most classified information. We cannot let that happen. It is more effective, much easier, much less expensive to invade our information systems than it is to drop bombs on our large cities and power systems.

I have been encouraged by the level of cooperation that the business community wants to express, wants to participate in. But if they have that concern, then we need to respond and to make it clear, to underscore, to clarify that they can exchange that information without fear of protracted litigation and exposing even greater vulnerabilities.

So, it is a good piece of legislation. I am glad the vast majority of witnesses on the panel agree. I certainly appreciate your having the hearing, Mr. Chairman. I trust that we are going to be able to get the bill on the floor in an expedited fashion. Thank you, Mr. Horn.

Mr. HORN. We thank you. Since I am not a lawyer, and having listened to this discussion, I suggest we put a simplification in one of the findings that this is the Lawyer's Relief Act of the year 2000. [Laughter.]

I now yield to Mrs. Biggert for 10 minutes for questioning.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Mr. Tritak, in your outreach efforts to coordinate with the private sector and initiate public-private partnerships, what hurdles have you run into? For example, does the fear of the Federal law enforcement community hinder your ability to work with the private sector in addressing cyber security problems before they occur?

Mr. TRITAK. No, I would not say that law enforcement interferes with that activity. The fact is that the relationships between the Federal Government and private industry vary from sector to sector and company to company. There are many companies who feel very comfortable in an information exchange arrangement with Federal law enforcement, and a number of companies that participate in the National Infrastructure Protection Center exchange that kind of sensitive information.

There are others who are concerned that sharing information with the Government could precipitate investigations which can have an impeding effect on their ability to conduct business. And that is a hurdle that they view exists. Again, I think it is one of these things where when those kinds of concerns are expressed

they need to be taken seriously to get to the core of what the problem may be.

What I find very interesting, of course, is that when someone talks about whether industry is interested in dealing with Government, I think you cannot make it a broad statement because, for example, sometimes you may find companies feel more comfortable dealing with, let's say in the information technology area, dealing with the Commerce Department or dealing with the Defense Department, and others by tradition, for example the electric power industry, they have had very good, strong working relationships with Federal law enforcement well before the Information Age. So I think it depends—it depends on the culture of the industry, it depends on the nature of the type of information you are dealing with.

Clearly, the roles and responsibilities at different agencies need to be defined over time. We are introducing a new, changing technology that is going to transform the way we all live, the way we do government, and the way we do business. I am sure that over time the respective roles of different governments and agencies are going to have to reflect that. And I think that as those adjustments are made, you will deal with some of the issues that you have just raised, about industry's reluctance in certain cases and proactivism in others to deal with government will be redressed.

Mrs. BIGGERT. Is there any fear that if there is more coordination then between the agencies of the Federal Government that this might affect how companies would deal with it? Because information that they might feel comfortable about, for example, with the Commerce Department would be available to another agency.

Mr. TRITAK. I think some have that concern, not all though. But some, yes.

Mrs. BIGGERT. Then version 1.0 of the President's National Plan for Information Systems Protection discusses the possibility that companies wishing to discuss possible systems vulnerability with the Federal Government may "be deterred from doing so because of the possibility that information disclosed to the Government could become subject to a request for public disclosure under" what we have been discussing, "the Freedom of Information Act."

Mr. TRITAK. That has been a concern expressed by some companies, yes.

Mrs. BIGGERT. Can you provide an estimate of how much private sector information is being withheld as a result of this?

Mr. TRITAK. I cannot say. I think to the extent that it has an inhibiting factor, it is the perception in certain cases that if the information may be used for reasons other than to help raise the level of security of the Nation's infrastructure is because it would become available to help address problems, that it can have a chilling effect. And depending on the companies and depending on their concerns, you never get to the point of deciding whether or not to give the information because your natural position is simply not to pass it on. And so it is hard to quantify. But I will say that it has been expressed and it has been expressed sufficiently so that I think it is not an isolated instance.

Mrs. BIGGERT. Thank you.

Ambassador Johnstone, are private sector participants concerned about the threat of law enforcement investigations hindering their ability to deliver critical services?

Ambassador JOHNSTONE. Actually, I do not disagree with Mr. Tritak. That is to say it is something that I have heard expressed. But in the many, many companies that I have talked to about this whole issue, that has not been high on people's agenda, the concern over law enforcement per se.

I think the fear of the loss of proprietary information, the fear of public disclosure of information that would not otherwise become public, the concern, and perhaps this touches on law enforcement, that people might not be exempt from sort of monopoly building kind of activities cause some level of concern.

The antitrust side of the equation. An American company, and I will speak from my own experiences having run an American company for a number of years, whenever you sit down with competitors you are surrounded by a galaxy of lawyers who are constantly looking at the antitrust implications of what you might do, even what you might do related to safety procedures and things of that type. And so there is a great deal of concern in terms of the antitrust implications. It would be a great relief to companies to have some relief from those concerns. I think public disclosure is certainly another area.

In terms of law enforcement and people's fear of being the subject of persecution, for example, that I have not actually encountered in terms of any individual contacts that I have had with businesses.

Mrs. BIGGERT. So there might be the concern about the law enforcement but you cannot really assess how much there is.

Ambassador JOHNSTONE. I think that concern is less than the concerns in the other areas.

Mrs. BIGGERT. Then does the partnership work with private sector on networks to disseminate information in a timely manner on potential vulnerabilities from sector to sector?

Ambassador JOHNSTONE. Well let me just say that the partnership got kicked off this last December in the first meeting in New York. We then hosted at the U.S. Chamber of Commerce a meeting of the partnership in the month of February and the next meeting is in July. So it is fairly embryonic and is just in its startup mode.

That being said, it certainly is the intent of the partnership, and certainly of the ISACS, to provide a maximum flow of information that will touch very much on the whole issue of network securities.

Mrs. BIGGERT. So this really is a goal of the partnership?

Ambassador JOHNSTONE. Certainly.

Mrs. BIGGERT. OK. Then would you be willing to share information with the Federal Government when uniform legal principles are established to structure the boundaries of a public-private partnership?

Ambassador JOHNSTONE. We would be willing to participate with the Federal Government on all aspects of working together to advance and to help protect the critical infrastructure, both when it comes to legislation as well as to working within the administrative framework.

Mr. TRITAK. If I may, Congresswoman.

Mrs. BIGGERT. Certainly.

Mr. TRITAK. Just a point of clarification. What the partnership, as I indicated in my testimony, aims to do is to encourage cross-sectoral dialog and activity to bring the owners and operators together, bring together other stakeholders involved. If the industry participants in that activity decide that it makes sense to create information-sharing arrangements amongst themselves, the partnership is one form in which that would be discussed, debated, and created. I think it is important though that the partnership itself is a forum to bring these issues to the fore for discussion. It is not in itself a super ISAC. It is not an organization that actually would do that as much as it would facilitate that development.

Mrs. BIGGERT. Thank you.

And I cannot not ask Mr. Willemssen a question since he has been at so many of our hearings. So, Mr. Willemssen, could you tell us to what extent the regulations that exist within the Federal law enforcement community and with the Federal Government for reporting on the cyber attacks or threats or vulnerabilities, how do they overlap?

Mr. WILLEMSSEN. There are some overlaps from an organizational standpoint. I would concur with Mr. Tritak's comments that there is a need for further definition and specificity on roles and responsibilities of Federal organizations so that the sectors and the private firms within those sectors know exactly who they are to deal with, what kind of information is going to be requested of them, what is going to be done with that information from an analysis perspective, and how the results of that analysis are going to be disseminated to others. Right now, that specificity does not exist. I know that Mr. Tritak and others are working on that and we would encourage them to continue doing that. That is definitely needed.

Mrs. BIGGERT. So right now this overlap is really hindering the ability to deliver or exchange information?

Mr. WILLEMSSEN. Yes. I think to the extent that further clarification can be provided, possibly in the next version of the National Plan which is due out this fall, that would be most beneficial to private sector.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. I thank the gentlewoman from Illinois.

I just have two questions here and then I will turn it over to all of you again.

This is directed at Mr. Willemssen. The General Accounting Office has commented extensively over the past 5 years on the number of problems confronting the Federal Government on addressing information security issues governmentwide and from agency to agency. In your view, Mr. Willemssen, does the lack of coordination and planning within the executive branch of the Government hinder its ability to be an effective cyber security partner in monitoring potential threats?

Mr. WILLEMSSEN. I think the lack of coordination has been a hindering factor. But I think there is a much bigger factor at play as it pertains to Federal agencies, and that is basic management of computer security issues. The Federal Government currently does

not have its house in order on computer security and protection of its systems and data.

So coordination is definitely an issue. But what we would like to see are individual agencies taking computer security much more seriously than they have in the past and making sure that they have done the risk assessments, they have adequate protection in place, they have made their staff very aware of the criticality of this issue, and there is an overall central guiding management to make sure that it is a priority within the agency.

Mr. HORN. Has the General Accounting Office ever had a request from the Article III Judiciary on this area? I would think there is some mischief that could be made in that area.

Mr. WILLEMSSEN. We do currently have a request looking at critical infrastructure from a Senate Judiciary Subcommittee. That work is ongoing.

Mr. HORN. In relation to the Article III Judiciary?

Mr. WILLEMSSEN. I do not believe it specifically covers that. But if I may, Mr. Chairman, get back to you and answer that for the record.

Mr. HORN. You might want to talk with the Administrative Office of the U.S. Courts and see what is happening.

Mr. WILLEMSSEN. Yes, sir.

[The information referred to follows:]

Our ongoing work on critical infrastructure protection does not address article III-related entities.

Mr. HORN. The General Accounting Office has offered its view in support of the creation of a Federal Chief Information Officer, a CIO that would centrally manage information technology, including information security, in its comments on Senate bill S. 1993. In your view, would a central coordinating office within the Federal Government on critical infrastructure protection that would work with both the public and private sectors overcome some of the similar obstacles to management and overlapping regulation that you have mentioned?

Mr. WILLEMSSEN. We are supportive of a strong central CIO position. In addition, we think, and it is instructive to look at Y2K as a lesson here, top management attention to a critical national issue is absolutely invaluable in making sure that the issue is adequately addressed in working with the public and private sector.

So to the extent that an overall national coordinator can help fill that role, we think that would be beneficial. But to the extent that it is a separate position, we need to make sure that it works with the institutions in place that have an overall focus on CIO issues. I do not think you can take a critical infrastructure and computer security and put it off on the side necessarily. You still have to work in tandem with overall management of information technology.

Mr. HORN. Well, it is an interesting view and we might be discussing this in the next few weeks because we have a few thoughts on the institutional aspects of the Presidency and how you relate to the departments. So I thank you for that view, and there might be a few other views.

Let me ask my colleagues here, the gentleman from Texas, do you have some more questions you would like to ask?

Mr. TURNER. I have no further questions.

Mr. HORN. The gentleman from Virginia?

Mr. DAVIS. No questions.

Mr. HORN. The gentlewoman from Illinois? No?

There might be a few questions we will send you and we would appreciate it if you could just bat us out a simple answer to complete and round out the record.

We again thank you for doing the last minute in a hurry. I suspect you were like the students in their senior year, they want to graduate and they stay up all night. So thank you for your energy and thank you for your wisdom on this. We appreciate it very much.

I now want to thank the staff for both the majority and the minority. On my immediate left, your right, is J. Russell George, the staff director and chief counsel of the Subcommittee on Government Management, Information, and Technology; Bonnie Heald, the director of communications, is in the back; Bryan Sisk, our clerk; Will Ackerly, intern; Chris Dollar, a new intern; and Meg Kinnard, a new intern. With Mr. Turner's staff, Trey Henderson is the counsel; Jean Gosa is the minority clerk. And our official reporter of debates, whom we thank, is Elisabeth Lloyd. And we have Mr. Davis' staff has done some excellent work, and I know that from working with them over the last few months, and that is Melissa Wojack and Amy Herrick. We thank you for all the work you have done on this legislation.

If there are no further questions, we thank you all.

Mr. DAVIS. Mr. Chairman, let me just add that if anyone on the committee would like to serve as a cosponsor as this bill moves up, we would happy to put your name on it.

Mr. HORN. OK. Thank you.

We will now adjourn this hearing.

[Whereupon, at 11:53 a.m., the committee proceeded to other business.]

[Additional information submitted for the hearing record follows:]

NAM National Association of Manufacturers

Marshall E. Whitenton
Vice President
Resources, Environment, and Regulation

June 20, 2000

The Honorable Steve Horn
Chairman
Subcommittee on Government Management, Information and Technology
House Committee on Government Reform
U.S. House of Representatives
B-373 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

The National Association of Manufacturers (NAM) welcomes the hearing on H.R. 4246, the Cyber Security Information Act. The NAM -- 18 million people who make things in America – is the nation's largest and oldest multi-industry trade association. The NAM represents 14,000 member companies (including 10,000 small and mid-sized companies) and 350 member associations serving manufacturers and employees in every industrial sector and all 50 states.

The NAM affirms the findings and premises behind this bill. One cannot responsibly disregard the possibility that the same hostile powers or groups that would blow up a U.S. aircraft, or attack a U.S. embassy or federal office building, would also seek to inflict damage by a computer-related attack. The NAM has commended President Clinton for his critical infrastructure protection initiative.

Already, Congress has decided that protection against terrorism requires an adjustment to the Freedom of Information Act (FOIA). In last year's Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRA), Congress removed parts of certain reports mandated under Section 112(r) of the Clean Air Act from FOIA release. Specifically, the hypothetical off-site consequence analyses submitted to the Environmental Protection Agency (EPA) by thousands of chemical-producing and -using facilities – or "worst case scenarios" – will now be available in limited format and numbers. The intent is to prevent terrorists from reconstructing a "hit list" of facilitates whose attack would result in the greatest number of casualties (see the joint proposed rule from the EPA and the Department of Justice, 65 *Federal Register* 24834, April 27, 2000).

The June 22 hearing is therefore very timely. Even with last year's welcome legislation – passed by Congress just as the deadline for response to FOIA requests immediately submitted to EPA had arrived – the FOIA status quo cannot be called satisfactory. Agencies have discretion to withhold cyberthreat information voluntarily submitted by industry but are not required to do so. Strong guidance to agencies from the Department of Justice would certainly help. A statutory enactment would be even more forceful.

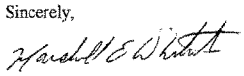
The NAM appreciates and values the FOIA. Indeed, the NAM files FOIA requests itself from time to time and agrees that this legislation should not narrow the FOIA beyond the minimum amount necessary to accomplish the key objectives of the critical infrastructure initiative. However, in our view, companies cannot be expected to reveal their vulnerabilities or losses without the greatest confidence that the information will not leave the hands of the government agency or agencies involved. That confidence simply does not now exist.

H.R. 4246 offers one approach to amending the FOIA. The NAM can support it as introduced. At the same time, the NAM is willing to consider supporting other drafting approaches. The drafting challenge is to create the conditions of confidence for industry, while reassuring groups traditionally supportive of the FOIA that the new provisions will not be misused.

The NAM also supports the antitrust exemption provided by H.R.4246. Just as with the successful National Security Telecommunications Advisory Committee, now 18 years old, many companies will have to work together. Removing the cloud of uncertainty about possible antitrust liability will reduce legal costs, improve information flow and promote the goals of the critical infrastructure protection initiative.

The NAM is an active partner in the Critical Infrastructure Partnership and looks forward to working with the subcommittee as the legislation progresses. For further information, you may contact David Peyton, director, technology policy, (202) 637-3147, dpeyton@nam.org; Larry Fineran, assistant vice president, resources, environment and regulation, (202) 637-3174, lfineran@nam.org; or myself.

Sincerely,



Marshall E. Whitenton
Vice President
Resources, Environment and Regulation

cc: The Honorable Thomas Davis, III
The Honorable James Moran

**From:** George, Russell
**Sent:** Wednesday, June 21, 2000 6:36 PM
**To:** Bryan Sisk
**Subject:** FW: Davis/Moran Bill

foia hill cover

admin ltr signed.doc 1

Davis Moran 1

ATT28518.txt

More letters for the Members's packets

-----Original Message-----
From: Wojciak, Melissa
Sent: Wednesday, June 21, 2000 6:23 PM
To: George, Russell
Subject: FW: Davis/Moran Bill

-----Original Message-----
From: Kaplan, Randy
Sent: Monday, June 19, 2000 4:25 PM
To: Russell George; Melissa Wojciak
Subject: FW: Davis/Moran Bill

-----Original Message-----
From: Ari Schwartz [mailto:ari@cdt.org]
Sent: Monday, June 19, 2000 2:29 PM
To: Bailey, Heather
Cc: Kaplan, Randy; Deirdre Mulligan; Jim Dempsey
Subject: Davis/Moran Bill

Heather,

Here are three letters on the Davis Moran bill. The first is a cover letter that we sent to members of the Senate Judiciary Committee introducing a letter to the administration that was signed by 19 groups expressing concern over the bill. The third document is CDT's memo on the bill.

I have not seen the witness list, but Steve Aftergood from the Federation of American Scientists; Kate Martin of the Center for National Security Studies; or Patrice McDermott (who also has a memo on this issue) would all be very good witnesses. Jim Dempsey from our staff would be good as well, but he is in France until Thursday morning.

I'm headed out of town until Thursday Morning, if you'd liek to follow up please call my cell phone 202-256-0914.

Thanks

Ari

PS - the time of this hearing on the Web site is listed as 10 PM.

---

June 6, 2000

The Honorable Orrin G. Hatch

Chairman
Senate Judiciary Committee
224 Dirksen
Washington, DC 20510

Dear Chairman Hatch:

Attached is a letter from 19 public interest organizations opposing any wholesale exemption from the Freedom of Information Act for information shared by industry with the government regarding vulnerabilities either in computer security systems or in other infrastructures.

The attached letter is addressed to the Administration, but we wanted to apprise you of these concerns because some Senators have also expressed interest in drafting legislation on this FOIA issue, and it may come up in the course of consideration of your bill, S. 2448, or other legislation within the jurisdiction of the Judiciary Committee.

As the attached letter indicates, there is certain information about specific vulnerabilities of specific infrastructures, which is largely irrelevant to public policy, and which, if disclosed would be likely to cause concrete harm. However, much of this information is already exempt from the FOIA. Before enacting any new legislative exemption to FOIA, the Administration and the Congress should conduct a careful inquiry, specifically identifying any additional information that needs to be exempted from disclosure and weighing the benefits to the public interest in knowing the specific information against any likely harm from disclosure.

We would be happy to discuss these concerns further with you or your staff.

Sincerely,

Kate Martin
Director
Center for National Security Studies

James X. Dempsey
Senior Staff Counsel
Center for Democracy and Technology

Steven Aftergood
Project Director
Federation of American Scientists

---

June 6, 2000

John Podesta
Chief of Staff
The White House
Washington, D.C. 20500

Dear Mr. Podesta:

We are writing to express our serious concern about various proposals being discussed to create a wholesale exemption from the Freedom of Information Act for information relating to critical infrastructures. We are opposed to any wholesale exemption for information shared by industry with the government regarding vulnerabilities either in computer security systems or in other infrastructures.

The idea for such an exemption was mentioned, without elaboration, in one line in the Report of the President's Commission on Critical Infrastructure Protection. We have become aware of various ad hoc efforts within the Administration to draft a wholesale exemption for such information; we are Iso aware that there are similar efforts in the Congress. This approach is rundamentally inconsistent with the basic premise of the Freedom of Information Act: the public in a democratic society must be informed about the activities of its government.

It is clear that, as we enter a new century, the government will focus more and more on the protection of critical infrastructures. Increasingly, government business will be conducted in cooperation with the private sector and, accordingly, will involve extensive sharing of information between the private sector and government. The current proposals all contemplate an automatic wholesale exemption from the Freedom of Information Act for such information. Such an exemption would hide from the public essential information about critically important government activities. Moreover, the most likely result will be weaker, not stronger, protection for infrastructures.

We recognize that there is certain information about specific vulnerabilities of specific infrastructures, which is largely irrelevant to public policy, and which, if disclosed would be likely to cause concrete harm. Much of this information is already exempt from the FOIA. For example, information concerning the software vulnerabilities of classified computer systems used by the government and by defense contractors is already exempt under (b)(1); the exemption in (b)(4) for trade secrets and confidential information also provides extensive protection from disclosure.

The Administration should follow the usual process for considering a new exemption if it is concerned that additional specific information needs to be exempted from disclosure. Individual agencies should identify any such information they may receive from industry. It can then be determined whether the information is already exempt. If the information is not exempt, a specific exemption can be proposed followed by a public debate regarding the need for an exemption, weighing the benefits to the public interest in knowing the specific information against any likely harm from disclosure. Such a process is currently underway at the Federal Aviation Administration regarding an exemption for some voluntarily-submitted industry information. While this approach requires some time and effort, it is necessary to meet the fundamental requirement of the Freedom of Information Act that information in the hands of the government presumptively must be public.

Finally, it is irresponsible to believe that only a wholesale exemption will satisfy industry fears. Industry and government are already cooperating and sharing information concerning how to protect infrastructures; we have no doubt this will continue. But such sharing cannot serve as the occasion to fundamentally rewrite the rules on how public policy is made and implemented in a democracy - that information used by and relied upon by the government is presumptively open to the public, whatever its source.

This Administration's commitment to a strong Freedom of Information Act repeatedly has been demonstrated since its early days. We urge you now to reject any calls for a wholesale exemption and instead to commit to a process consistent with the principles of open government embodied in the FOIA.

Sincerely,

Kate Martin
Director
Center for National Security Studies

James X. Dempsey
Senior Staff Counsel
Center for Democracy and Technology

Thomas S. Blanton
Executive Director
National Security Archive

Robert S. Norris
Natural Resources Defense Council

Anders Gyllenhaal
Freedom of Information Chairman
American Society of Newspaper Editors

Patrice McDermott
OMB Watch

Steven Aftergood
Project Director
Federation of American Scientists

Lucy Dalglish
Executive Director
Reporters Committee for Freedom of Press

Daniel Plesch
Director
British American Security Info Center

Mary Alice Baish
Associate Washington Affairs Rep
American Association of Law Libraries

Greg Nojeim
American Civil Liberties Union

Conrad Martin
Fund for Constitutional Government

Amanda Frost
Public Citizen

Harry Hammitt
Access Reports

David Sobel

Charles J. Sanders

General Counsel
Electronic Privacy Information Center

James Madison Project

Terry Greene
JSI Center for Environmental Health Studies

Michael Gregory
Director
Arizona Toxics Information

Stephen M. Brittle
President
Don't Waste Arizona, Inc.

---

May 2000

Davis-Moran Cyber Security Information Act - H.R. 4246

CDT Analysis

The bill has four main components: an antitrust exemption, a FOIA exemption, a disclosure and use limitation, and an exemption from the Federal Advisory Committee Act. The first is easily dealt with: The antitrust exemption, Sec. 6 of the bill, is probably as harmless as it is unnecessary, although the Antitrust Division may worry that the exception to the exemption, Sec. 6(b), by being too narrow, creates an implication that the exemption is broader than intended.

The FOIA and disclosure/use issues are far more complicated. They are quite separate issues too: While the FOIA exemption has attracted the most attention, and while the assertion of need for the bill is based on stated concerns that the FOIA will expose to terrorists and hackers vulnerabilities in power grids and other key infrastructures, the disclosure/use limitations are limits on the government and on other businesses. They are very broad and, as drafted, could have many unforeseen consequences, including unintended negative effects on the very companies they are meant to protect.

What is the national goal: immunity or accountability?

The disclosure and use limitations, which are intended to shield companies from liability exposure based on shared information, seem to run counter to other cyber security initiatives that seek to use the liability/insurance system, auditing standards, and disclosure processes such as those of the SEC to promote accountability and therefore encourage cyber security remedial measures.

FOIA Issues:

Is the government the clearinghouse?

Some of the questions posed by H.R. 4246 stem from the fact that it is not clear what model for information-sharing it seeks to promote: will a government agency serve as the information clearinghouse, or will the sharing occur within industry. The sponsors of the bill cite the industry ISAC ("information sharing and analysis center") model. But the financial services industry has created an ISAC without FOIA concerns since the government is not a participant and therefore nothing is subject to FOIA.

Sharing versus nondisclosure

Whether or not the government is the clearinghouse, the bill's drafting raises a host of questions: The bill says that, except with the express consent or permission of the provider, covered information "shall not be disclosed to or by any third party." Sec. 4(c)(2). This basically gives the submitter of the information control over its use and disclosure. Presumably, most submitters would specify that the information could be disclosed to other members of a trusted network. The bill doesn't say who will decide who is in and who is outside that network. With respect to vulnerabilities in widely-used computer systems, limiting disclosure to a small network poses a risk that the information will not get to all those who would benefit from it. It is one thing for industry to form sectoral or regional sharing systems - it is different to enshrine non-disclosure as a Federal legal mandate.

A "submitter controls" approach has appeal, but it poses some problems. What if information is submitted anonymously, so that the recipient (governmental or not) cannot go back and seek permission to disclose? This would mean that the recipient would be prohibited from disclosing this information even to the intended target of an attack. Similarly, if the information comes from an informant, who said he didn't want it disclosed, again the government would be precluded from overriding the desire of the informant, even to the extent of sharing the information with the intended target.

Could the nondisclosure and nonuse provisions prevent companies from defending themselves against false accusations? If a claim is made that Windows has a vulnerability, doesn't Microsoft deserve to know that somebody is claiming that its product is faulty? Shouldn't the government be able to share that allegation with Microsoft and get Microsoft's response? Yet under the bill, if the submitter of vulnerability information gives consent to share it with anybody except Microsoft, that restriction controls.

If the allegation is untrue, shouldn't Microsoft be able to seek remedies against the person who disparaged its product? The civil litigation prohibition restricts Microsoft and other companies from defending themselves against false allegations.

Do the nondisclosure and nonuse provisions preclude standard contract remedies? For example, if a government vendor admits that one of its systems is insecure, shouldn't the government agency that has a contract to purchase and use the system be able to cancel its contract and defend itself against a breach of contract suit on the ground that the supplier admitted that the system was insecure? Yet Sec. 4(c)(3) says that the information may not be used by any Federal or State entity, agency of authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law.

Definitions: What information is covered?

A very difficult issue is defining what information is covered.

A central term in the bill is "cyber security statement," defined as "any communication Š by a party to another, in any form or medium including ... a website Š concerning the cyber security of that entity." Sec. 3(5). On the one hand, that seems too narrow, since, if the words "of that entity" refer to the party making the statement, the bill would not include a statement by one entity about the cyber security of another entity. Thus,

if a security expert finds a flaw in the system or program or another company, and warns the government, that information is not covered, since it is not a statement about the cyber security of the entity making the communication. Also not covered are in-house assessments that are not communicated "to another." Therefore, if the FAA discovers a vulnerability in its air traffic computers but doesn't tell "another," the information sitting in the FAA files is still subject to FOIA.

Compounding this problem, the bill only covers "cyber statements or other such information provided by a party in response to a special cyber security data gathering request made under this section." This means that any information not communicated "in response to a special cyber security data gathering request" is not covered. Unless every Federal agency with CIP responsibilities immediately issues a blanket special data gathering request for any and all cyber security information, this will create confusion as FOIA processors try to determine whether cyber security information was obtained in response to a designated request or came into the government's possession independently. This provision may actually curtail disclosure to the government, since companies may hesitate to share cyber security information with agencies that have not issued "special cyber security data gathering requests." Also, the bill doesn't seem to cover information in government files before date of enactment, since it would not be information provided in response to a "special cyber security data gathering request made under this [bill]."

On the other hand, the definitions seem overbroad. They cover "any communication by a party to another Š concerning an assessment Š concerning the cyber security of that entity, its computer systems, its software programs Š or commenting on Š the cyber security thereof." This means that a statement by a Microsoft engineer commenting on a news report about an alleged security flaw in Windows is a covered "cyber security statement." It is subject to the restrictions of the bill "except with the express consent or permission of the provider." Does that mean that one hearing that comment shall not disclose it unless the engineer expressly gave permission to do so?

The bill includes statements posted on cyber secu.ity Internet website, a defined term. Sec. 3(4). There are hundreds, perhaps thousands, of such sites in existence now, run by the FBI < http://www.fbi.gov/nipc/nipcaaw.htm>, the CERT at Carnegie-Mellon, Cisco <http://www.cisco.com/warp/public/707/advisory.html>, L0pht <http://www.l0pht.com>, and many others. Attrition.org lists 3027 onsite and offsite security advisories: <http://www.attrition.org/security/advisory/>. There is no reason to cover these and then exempt them under the public disclosure exception of Sec. 4(d)(2). (The exception requires "the express consent of the party." Is that the express consent of the party owning the system to which the information relates, the party making the statement, or the party posting it online?) Anyhow, as pointed out below, the website provision is drawn from the Y2K Act, where it served a very different function. It is inapplicable here.

Any Federal agency may expressly designate a request for information as a "cyber security data gathering request," but the bill goes on to say that a cyber security data gathering request "shall be a request from a private entity Š to a Federal entity." It goes further to say that a cyber security data gathering request "shall be deemed to have been made Š when the Federal entity Š has voluntarily been given cyber security information gathered by a private entity Š including by means of a cyber security Internet website." This seems to say that "a cyber security data gathering request Š shall be deemed to have been made" whenever the government is given information. Is the government "given" information when it is published on a website, printed in the newspaper, sent to a government employee who subscribes to a cybersecurity mailing list, or otherwise provided to the government?

Is the bill necessary?

The Justice Department has determined that it could successfully defend against FOIA requests for cyber security information under the (b)(4) FOIA exemption for proprietary information. See Critical Mass Energy Project v.

Nuclear Regulatory Commn, 975 F.2d 871, 880 (D.C. Cir. 1992 (en banc), cert denied, 507 U.S. 984 (1993) ("Exemption 4 protects any financial or commercial information provided to the government on a voluntary basis if it is of a kind that the provider would not customarily release to the public."). In some cases, the FOIA exemptions for national security information (b)(1) and law enforcement information (b)(7) would also be available.

But some argue that the bill is necessary to overcome industry reluctance (however unjustified legally) to share information with the government. Yet given the issues raised above, a FOIA exemption and/or a disclosure and liability exclusion could serve to shield information that one party in a business-to-business dispute would want to obtain and use.

Y2K precedent not applicable

H.R. 4246 is loosely, but only loosely, patterned on the Y2K Information and Readiness Disclosure Act, Pub. L. 105-271. The Y2K Act addressed such a different problem and from such a different perspective that it is probably not a useful model for the cyber security issue. Y2K involved a known problem that was going to cause unpredictable damage unless fixed. It made no sense to hide the problem out of fear that it could be exploited by terrorists. The main focus of the Y2K Act was liability associated with the disclosure and exchange of Y2K readiness information. FOIA was a minor concern. The goal was not to keep Y2K information secret, but to disclose it, so the public could know whether the problem was being solved.

Compare the purposes section of the Y2K bill ("to promote the free disclosure" of Y2K information and "to assist consumers, small businesses and local governments") with the purposes section of H.R. 4246 ("to promote the secure disclosure" of cyber security information and "to assist private industry and the government") (emphasis added). Compare also Sen. Bennett's statement on introduction of the Y2K legislation, where he explained that the Y2K bill "attempts to limit the legal liability of corporations and other organizations who in good faith openly share information about computer and technology processing problems and related matters in connection with the transition to the Year 2000." (Emphasis added.) Similarly, lead co-sponsor in the House, Rep. Eshoo, said: "This legislation frees organizations to communicate more openly with the public and, just as importantly, with each other, about the status of Year 2000 work on critical systems." (Emphasis added.)

The Y2K bill ended up as a very complicated law of short term duration. There are many details in the Y2K Act missing from H.R. 4246. Most notably, theY2K Act's FOIA exemption stated that Y2K statements were exempt under (b)(4) of the FOIA, the exemption for proprietary data, while H.R. 4246 contains no reference to (b)(4). A bill that fits within the preexisting framework of exemption (b)(4) is less likely to given an overbroad interpretation than a free-standing or (b)(3) exemption.

For further information, contact Jim Dempsey (202) 637-9800 jdempsey@cdt.org

SENT BY: 6-21- 0 ; 6:24PM ; DC SUBCOMMITTEE→ 202 225 2373;# 1/ 1
National Journal's Technology Daily

to Russell Kunge: 5-2373

White House

## WH Leans Toward House Cyber Security Plan

The Clinton administration supports efforts aimed at encouraging information sharing about cyber security among companies and the federal government by providing some liability protection from antitrust laws and the Freedom of Information Act, an administration official said Wednesday.

While praising legislation offered by Reps. **Tom Davis**, R-VA, and **James Moran**, D-VA, **Jeffrey Hunker**, senior director of critical infrastructure protection at the National Security Council, stopped short of endorsing the bill, H.R. 4236. He did say, however, that the administration has been working with the lawmakers and it is discussing ways to address some technical areas of concern.

ops!

**Quote of the Day**

"It could help change the most sophisticated surveillance mechanism on the planet to something that we can all be comfortable with surfing."

*— Rep. Ron Paul, chairman of the subcommittee on the protection of privacy in cyberspace*

H.R. 4236, which will be the subject of a hearing Thursday before a House Government Reform Committee subcommittee, would exempt cyber security data from disclosure by federal agencies via the Freedom of Information Act and provide protection from antitrust laws when companies are cooperating on ways to address or avoid cyber security attacks.

Industry officials have expressed concern about sharing proprietary information about such attacks with the federal government for fear that it could be made public under FOIA or by discussing the issue among themselves they could run afoul of antitrust laws.

"Overall, were very supportive of the idea of promoting information sharing and recognize that concerns about the Freedom of Information Act are a major barrier to private industry working closely with the government," Hunker said at a conference on cyber security. "In general, were supportive of efforts to clarify and limit the liability that companies...have."

The conference, co-sponsored by the Virginia Bar Association, College of William and Mary Law School and two cyber security federal offices, focused on liability, security and privacy issues related to protecting computer networks from cyber attacks. Former Virginia Gov. **Gerald Baliles** said the Davis-Moran bill was brought up, but he declined to provide details about other liability issues discussed during the closed session attended by academics and industry and government officials. The conference focused on educating those involved on various issues and questions surrounding cyber protection so that industry and government can "begin to pull together information" about what public policy actions should be taken, Baliles said.

The free flow of information "can be jeopardized if these questions are not addressed," Baliles said.

Much of the conference focused on trying to clarify "basic legal issues" related to cyber security, said Hunker, who added that the administration plans to sponsor similar conferences in other parts of the country.

*- by Juliana Gruenwald*

Index

Taxes

## Internet Tax Moratorium Still Stalled In Senate

Legislation to extend the current moratorium on Internet taxes is still stalled in the Senate as the chairman of the Senate Commerce Committee works to