AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERTERRORISM: IS THE NATION'S CRITICAL INFRASTRUCTURE ADEQUATELY PROTECTED?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

JULY 24, 2002

Serial No. 107–217

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

87–387 PDF WASHINGTON : 2003

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

COMMITTEE ON 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
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma

HENRY A. WAXMAN, California
TOM LANTOS, California
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
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
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DOUG OSE, California
ADAM H. PUTNAM, Florida
JOHN SULLIVAN, Oklahoma

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
BONNIE HEALD, *Deputy Staff Director*
CHRIS BARKLEY, *Assistant*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on July 24, 2002	1
Statement of:	
Belcher, Timothy G., chief technology officer, Riptech, Inc.	15
Charney, Scott, chief security strategist, Microsoft Corp.	31
Dacey, Robert F., Director, Information Security Issues, U.S. General Accounting Office	70
Dick, Ronald L., Director, National Infrastructure Protection Center, Federal Bureau of Investigation	136
Jarocki, Stanley R., chairman, Financial Services Information and Analysis Center, and vice president, Morgan Stanley IT Security	159
Leffler, Louis G., manager-projects of North American Electric Reliability Council	165
Maiffret, Marc, chief hacking officer and co-founder, eEye Digital Security	60
Paller, Alan, director of research, SANS Institute	23
Thomas, Douglas, associate professor, Annenberg School for Communication, Los Angeles, CA	8
Tritak, John S., Director, Infrastructure Assurance Office, Department of Commerce	150
Weiss, Joseph M., executive consultant, KEMA Consulting	43
Letters, statements, etc., submitted for the record by:	
Belcher, Timothy G., chief technology officer, Riptech, Inc., prepared statement of	17
Charney, Scott, chief security strategist, Microsoft Corp., prepared statement of	34
Dacey, Robert F., Director, Information Security Issues, U.S. General Accounting Office, prepared statement of	72
Dick, Ronald L., Director, National Infrastructure Protection Center, Federal Bureau of Investigation, prepared statement of	139
Jarocki, Stanley R., chairman, Financial Services Information and Analysis Center, and vice president, Morgan Stanley IT Security, prepared statement of	161
Leffler, Louis G., manager-projects of North American Electric Reliability Council, prepared statement of	167
Maiffret, Marc, chief hacking officer and co-founder, eEye Digital Security, prepared statement of	62
Paller, Alan, director of research, SANS Institute, prepared statement of	26
Shakowsky, Hon. Janice D., a Representative in Congress from the State of Illinois, prepared statement of	5
Thomas, Douglas, associate professor, Annenberg School for Communication, Los Angeles, CA, prepared statement of	11
Tritak, John S., Director, Infrastructure Assurance Office, Department of Commerce, prepared statement of	152
Weiss, Joseph M., executive consultant, KEMA Consulting, prepared statement of	45

CYBERTERRORISM: IS THE NATION'S CRITICAL INFRASTRUCTURE ADEQUATELY PROTECTED?

WEDNESDAY, JULY 24, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Schakowsky.

Staff present: J. Russell George, staff director; Bonnie L. Heald, deputy staff director; Chris Barkley, assistant to subcommittee, Michael Sazonov, professional staff member; Sterling Bentley, Joey DiSilvio, Freddie Ephraim, and Yigal Kerszenbaum, interns; David McMillen, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

In 1998, a 12-year-old boy successfully hacked into computer systems that controlled the Roosevelt Dam in Arizona. He could have opened the dam's floodgates and dumped nearly 500 billion gallons of water on the Arizona cities of Mesa and Tempe. Fortunately, he did not.

However, in April 2000, an Australian hacker used his laptop computer and a commercially available radio transmitter to gain control of a local sewage treatment facility. He intentionally released raw sewage into nearby parks and rivers on 46 occasions before he was caught.

It is clear from these and other reports that the Nation's water, power, financial markets, and telecommunication systems could be similarly attacked. These systems are essential to the health and well-being of all Americans, and they are fundamental to the continued operation of the government. More than 90 percent of the Nation's critical infrastructure is owned and operated by the private sector. To protect these assets, it is important to understand their vulnerability to cyberattacks, which are increasing in intensity and sophistication.

During the first 6 months of this year, the Carnegie-Mellon CERT Coordination Center received reports of 43,000 cyberattacks.

In comparison, last year, the Center received approximately 53,000 reports of attacks for the entire year.

In many cases, businesses may not know when a cyber-attack is launched and may not gracefully recover from the attack. A recent survey of Fortune 500 companies by Ernst & Young found that only 40 percent of those companies were confident that they could detect an attack on their systems. The same survey also revealed that only 53 percent of the companies had business continuity plans to recover from an attack.

To shore up the defense of the Nation's critical infrastructure, each industry group has formed its own information sharing and analysis center. These centers face formidable challenges. The businesses within each sector can vary widely in size and complexity and in their ability to safeguard their systems.

For example, the financial service sector includes large banking corporations as well as small independent banks. Nevertheless, the financial sector center must develop common security processes in order to report, respond, and recover from a cyber-attack. Each center tends to focus on risks that are unique to its industry, even though the sectors are increasingly interconnected and interdependent. Damage to one can cascade to others. The recovery plans of one sector could affect the ability of other sectors to resume operation.

Today's hearing will examine the roles and limitations of the information sharing and analysis centers and will explore what actions may be needed to ensure the security of the Nation's infrastructure. I welcome today's witnesses, and I look forward to working with you on this vital concern.

Let me administer the oath, and then we will go into recess, because I believe we have a vote on the floor. So, if you will stand, raise your right hand.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all affirmed the oath.

Please sit down and relax. And we are delighted to have Ms. Schakowsky, the ranking member. And she will use her time to give her statement to open the hearing, and we will then go in recess.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

It is unfortunate that we are having this hearing today. The issue before us is an important one that should be given due consideration by Congress. But instead, the majority has insisted on circumventing regular order and is trying to move language on this issue as part of the homeland security bill, language that would probably not become law if considered separately and openly, and language that is designed not to improve public safety but to curry favor with the business community.

There is an attempt on the part of some to exclude from the Freedom of Information Act all information submitted voluntarily by businesses in the name of critical infrastructure protection. One of our witnesses today testified before the Senate that the government has the ability under the Freedom of Information Act and under almost 30 years of case law to protect information submitted voluntarily to the government by businesses. He goes on to say

that, "If the private sector doesn't think the law is clear, then by definition it isn't clear."

I am puzzled by that logic. I always thought it was the role of the courts and not the private sector to clarify the interpretation of the law. By this gentleman's logic, any law that businesses disagree with, they only have to claim it as unclear and it becomes incumbent on Congress to change that law. I wonder if that logic extends to individuals.

Mr. Chairman, I want to draw on the testimony David Sobel will be submitting for the record, and ask unanimous consent that his testimony be included in the record.

Mr. HORN. Without objection, it will be put in the record at this point.

Ms. SCHAKOWSKY. I also ask that the letter from Jim Dempsey at the Electronic Privacy Information Center be included the record.

Mr. HORN. Without objection, it will be in the record at this point.

Ms. SCHAKOWSKY. The fourth exemption to the Freedom of Information Act protects information which is a trade secret or information which is commercial and privileged or confidential. This information is considered confidential if disclosure of the information is likely to impair the government's ability to obtain the necessary information in the future or to cause substantial harm to the competitive position of the business from which the information was obtained.

Let me restate this because it is exactly the point that has been ignored by those seeking this exemption. The Freedom of Information Act protects information submitted by businesses if that information is confidential. That information is confidential if the release of the information would make it more difficult to obtain that information in the future.

The language in the Freedom of Information Act is quite clear. It doesn't end there. There are even more protections for confidential business information. In 1987, President Reagan issued Executive Order 12600, which provides notice to a business if the agency determines material submitted by that business and identified as confidential should be released, the business has an opportunity to make its case before the agency and before a court of law.

Furthermore, no proponent of this exclusion from the Freedom of Information Act has cited a single example where a Federal agency has disclosed voluntarily submitted data against the expressed wishes of the industry which had submitted the information.

On the other hand, the damage this exclusion could do is legion. The language included in the homeland security bill would allow businesses and agency officials to hide lobbying activities under this exclusion. Officials from energy companies could meet with Federal officials to craft government energy policy, and all of those conversations could be hidden from public view. This language would shield these companies from antitrust law. Even the Attorney General objects to that provision.

Mr. Chairman, we all agree that the government has substantial work to do to assure the protection of our critical infrastructure. I hope that today's hearing will move us down that path. Unfortu-

nately, the language included in the homeland security bill does little to improve the security of our critical infrastructure, but instead is about hiding information from the public.

Thank you, Mr. Chairman.

Mr. HORN. Thank you.

[The prepared statement of Hon. Janice D. Schakowsky follows:]

STATEMENT OF THE HONORABLE JAN SCHAKOWSKY
AT THE HEARING ON
CRITICAL INFRASTRUCTURE PROTECTION

JULY 24, 2002

Thank you Mr. Chairman. It is unfortunate that we are having this hearing today. The issue before us is an important one that should be given due consideration by Congress. Instead, the majority has insisted on circumventing regular order and is trying to move language on this issue as a part of the homeland security bill - language that would probably not become law if considered separately and openly, and language that is designed not to improve public safety, but to curry favor with the business community.

There is an attempt on the part of some, to exclude from the Freedom of Information Act, all information submitted voluntarily by businesses in the name of critical infrastructure protection. One of our witnesses today testified before the Senate that the government has the ability, under the Freedom of Information Act, and under almost 30 years of case law, to protect information submitted voluntarily to the government by businesses. He goes on to say that "if the private sector doesn't think the law is clear, then by definition, it isn't clear." I am puzzled by that logic. I always thought it was the role of the courts, not the private sector, to clarify the interpretation of the law. By this gentleman's logic, any law that businesses disagree with, they only have to claim it is unclear, and it becomes incumbent upon the Congress to change that law. I wonder if that logic extends to individuals.

Mr. Chairman, I want to draw on the testimony David Sobel will be submitting for the record, and ask unanimous consent that his testimony be included in the record. I also ask that the letter from Jim Dempsey at the Electronic Privacy Information Center be included in the record.

The fourth exemption to the Freedom of Information Act protects information, which is a trade secret, or information, which is commercial and privileged or confidential. This information is considered confidential if

disclosure of the information is likely to impair the government's ability to obtain the necessary information in the future, or to cause substantial harm to the competitive position of the business from which the information was obtained.

Let me restate this because it is exactly the point that has been ignored by those seeking this exemption. The Freedom of Information Act protects information submitted by businesses if that information is confidential. That information is confidential if the release of that information would make it more difficult to obtain that information in the future.

The language of the Freedom of Information Act is quite clear. It doesn't end there. There are even more protections for confidential business information. In 1987, President Reagan issued Executive Order 12600, which provides notice to a business if the agency determines material submitted by that business and identified as confidential should be released. The business has an opportunity to make its case before the agency, and before a court of law.

Furthermore, no proponent of this exclusion from the Freedom of Information Act has cited a single example where a federal agency has disclosed voluntarily submitted data against the express wishes of the industry, which submitted the information.

On the other hand, the damage this exclusion could do is legion. The language included in the Homeland Security Bill would allow businesses and agency officials to hide lobbying activities under this exclusion. Officials from energy companies could meet with federal officials to craft government energy policy, and all of those conversations could be hidden from public view.

This language would shield these companies from antitrust law -- even the Attorney General objects to that provision.

Mr. Chairman, we all agree that the government has substantial work to do to assure the protection of our critical infrastructure. I hope that today's hearing will move us down that path. Unfortunately, the language included in the Homeland Security bill does little to improve the security of

our critical infrastructure, but instead is about hiding information from the public.

Mr. HORN. And we are now in recess until 10:30. Thank you.

[Recess.].

Mr. HORN. The recess has ended, and we will have peace and quiet for about an hour and a half just to get your various agendas.

We will now start with Douglas Thomas, the associate professor of Annenberg School for Communication at the University of Southern California. We are delighted to have you here.

STATEMENT OF DOUGLAS THOMAS, ASSOCIATE PROFESSOR, ANNENBERG SCHOOL FOR COMMUNICATION, LOS ANGELES, CA

Mr. THOMAS. Thank you. I have a longer statement to submit for the record, and I would like to summarize my comments here.

Mr. HORN. Thank you. Because let me tell all of you, your full written view goes right into the record, without even having to say it, the minute I give your name and what you are now doing.

So, thank you very much, Mr. Thomas. We all had a chance when we got them last night—a little late—but it is a very fine job that all of you have done. So, Professor Thomas, if you can give a summary of 5 minutes, 8 minutes, something, so we can get to questions, we would appreciate it. Thank you.

Mr. THOMAS. Thank you, and particularly for inviting me to speak before you today.

My name is Douglas Thomas, and I am Associate Professor in the Annenberg School for Communication at the University of Southern California. My research focuses on the social and cultural impacts of new media and technology, with particular emphasis on the subculture of the computer underground. I have recently published a book called Hacker Culture about the computer underground, and co-edited another called Cybercrime: Law Enforcement, Security and Surveillance in the Information Age.

For the past 7 years I have studied computer hackers in an effort to understand who they are, what motivates them, and how their culture can be understood in relationship to technological innovation. During that time, I have met with, spoken to, and interviewed hundreds of computer hackers, and I've spent time immersed in their literature and their culture, and I feel confident in saying that I understand for the most part how they think.

I would like to start off by answering the broad question: What are the risks that a terrorist organization might seek out hackers and employ them to carry out attacks on our information infrastructure?

With the vast majority of computer hackers, I would say upwards of 99 percent of them, the risk is negligible for the simple reason that hackers don't have the skill—those hackers don't have the skill or ability to organize or execute an attack that would be anything more than a minor inconvenience. Of the hackers that remain, my experience suggests that the most talented, who may be able to inflict serious damage, are neither inclined to do so nor likely to be tempted by financial incentives. They tend instead to be the most strongly motivated by an ethic which values security, which values information, and which puts innovation and learning at the top of those priorities. In other words, the idea of engaging in terrorism of any sort does not fit their profile.

In fact, I can think of few perspectives more hostile to radical Islamic fundamentalism than the ones that most hackers embrace. The typical hacker—and of, course, there are exceptions—is motivated by a profound sense of curiosity, by openness, by freedom and exploration. Hackers like to know how things work, and they like to make things work better or in unexpected ways. The hackers of today have a very clear ethic that shouldn't be overlooked by the committee. Above all else, they too believe in computer securities; and, most important, they believe that without constant vigilance, most software manufacturers will remain content to leave security as a secondary issue. They believe that in most computer software use today, security has become an add-on feature rather than a design principle; and it is that, above all else, which puts us at risk.

In a new age of corporate responsibility, it may be worth taking a few minutes to understand why hackers write programs that expose security flaws in computer software. Many hackers release public releases of security holes as a result of companies refusing to fix or oftentimes even acknowledge security flaws in their products primarily because there is no regulation for security in software, and, most important, there is no liability for software companies when their products create risks for consumers or the public.

At one level, the work that hackers do is not entirely unlike the work of a watchdog organization or Consumer Reports. Admittedly, the outlook, style, and demeanor are different, but the end results are the same. Hackers force computer software manufacturers to pay attention to security. We need to be careful to focus on the causes of such vulnerabilities and not blame the messengers.

When facing a question as weighty as cyberterrorism, a very serious problem that you face is getting the facts. I have yet to hear anyone articulate a realistic scenario in which computer hackers will be able to effect significant economic or physical damage in order to be considered a terrorist threat. It is easy to imagine scenarios that sound like terrorism: For example, hacking into air traffic control and crashing planes, or hacking into the stock exchange and undermining the stock market. These things make great Hollywood plots, but there is no evidence that any such scenario is possible, much less likely. In fact, most of the research I'm familiar with on this topic concludes the opposite.

For the foreseeable future, acts of cyberterrorism like the ones usually imagined, will be very difficult to perform, unreliable in their impact, and easy to respond to in relatively short periods of time. In point of fact, there has never been an act of cyberterrorism committed, nor has there ever been, to my knowledge, a computer hacking incident that has resulted in the loss of life. When these scenarios are proffered, I urge you to ask tough questions about them, about what additional security measures would have to fail for such an attack to take place.

Finally, I would like to conclude by saying that should a terrorist manage to launch a successful attack, it should be noted that our country has some of the best resources available to deal with it, diffuse, and neutralize such a threat. The faculty and students at places like MIT, Berkeley, Stanford, Purdue, Carnegie-Mellon, places like CERT and the NCSA, provide our best defense against

such threats, but these groups only provide that advantage as long as the network remains open and accessible. Security only gets better through testing, design, and redesign. The real threat to security is closing off avenues of exploration and examination. The more we know about our networks, the better we are able to defend them. It is that openness in testing which is essential.

So, as a result, I would encourage you to think of hackers not as the enemy but, instead, as an admittedly difficult-to-manage resource who may be in the best position to alert us of our vulnerabilities before they can be exploited.

Thank you, and I would be happy to take any questions you may have.

Mr. HORN. Well, we thank you. And we will get to the question period once we finish the whole panel.

[The prepared statement of Mr. Thomas follows:]

Testimony for the
Committee on Government Reform's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Cyber Terrorism and Critical Infrastructure Protection

July 24th, 2002

Douglas Thomas
Associate Professor
Annenberg School for Communication
University of Southern California
Los Angeles, CA 90089-0281

douglast@usc.edu

Good morning and thank you for inviting me to speak before you today. My name is Douglas Thomas and I am currently an Associate Professor in the Annenberg School for Communication at the University of Southern California. My research focuses on the social and cultural impacts of new media and technology, with a particular emphasis on the subculture of the "computer underground." I have recently published one book, *Hacker Culture*, about the computer underground and co-edited another, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, which explores a broad range of security issues from an international and comparative perspective. I have spent the past 7 years studying computer hackers, in an effort to better understand who they are, what motivates them, and how their culture can be understood in relation to technological innovation. During that time, I have met with, spoken to, and interviewed hundreds of computer hackers. I have spent time immersed in their literature and their culture and I feel confident in saying that I believe I understand, for the most part, how hackers think.

I want to address the question of our vulnerability, but I wish to do so from a perspective that you may have not heard before.

I'd like to start off by answering the broad question: what are the risks that a terrorist organization might seek our hackers and employ them to carry out attacks on our information infrastructure? With the vast majority of hackers, I would say 99% of them, the risk is negligible for the simple reason that those hackers do not have the skill or ability to organize or execute an attack that would be anything more than a minor inconvenience. Granted, hackers often have an antagonistic (and often times juvenile) response to authority, often producing behaviors that appear to pose a troublesome threat. As Steven Levy pointed out in his discussion of the role that hackers played in the creation of the PC and the information revolution, a central tenet to the "Hacker Ethic" has always been a profound mistrust of authority. Accordingly, today's hackers break into NASA and the Department of Justice web servers and rearrange their web pages. Occasionally, they even engage in Denial of Service attacks that make web sites inaccessible for brief periods of time. In short, they engage in behaviors that are typical of adolescent boys, challenging adult authority and flexing their muscles (in this case via technology) in the ways that young men (and in a relatively few cases, women) have done since time immemorial. It is a kind of vandalism that is and should be illegal. And when laws are broken, hackers should be caught, prosecuted and punished. But in times such as these, it becomes critical to ask ourselves what exactly the impact of computer hackers' behaviors is. Are these things annoying? Yes. Are they juvenile and occasionally embarrassing? Often. But are they dangerous? I don't think so. Certainly not at the level that you want to be discussing here today. I do not believe that terrorists are likely to attack us by knocking E-Bay offline for a few hours or that such an attack would constitute an act of cyberterror.

Of the hackers that remain, my experience suggests that the most talented, who may be able to inflict serious damage, are neither inclined to do so nor likely to be tempted by financial incentives. They tend instead to be the most strongly motivated by an ethic which values security, which values information, and which puts innovation and learning at the top of their list of priorities. In other words, the idea of engaging in terrorism, of any sort, does not fit their profile.

Here, it also might be of some use for me to discuss the hacker psychology. The typical hacker, and of course there are exceptions, is motivated by a profound sense of curiosity. Hackers like to know how things work and they like to make things work better or in unexpected ways. And while it may be convenient to divide the hackers of yesterday, such as Steve Jobs, Richard Stallman, Steve Wozniak, and Linus Torvalds from the hackers of today, doing so misses an important commonality. Hackers like innovation. They like identifying and finding elegant solutions to complex problems. Like the hackers of yesterday, the hackers of today have a very clear ethic that shouldn't be overlooked by this committee: Above all else, they too believe in computer security. And, most important, they believe that without constant vigilance most software manufacturers will remain content to leave security as a secondary issue. They believe that in most computer software used today, *security has become an "add on" feature rather than a design principle and it is that, above all else, which puts us at risk.*

In our new age of corporate responsibility, it may be worth taking a few minutes to examine one of the primary reasons that hacker are seen as threatening and why we might be quick to make associations between hacker activity and terrorist activity. Most of what hackers do is write programs that *expose security flaws* in computer software, mainly in the operating systems produced by Microsoft and to a lesser degree by Sun Microsystems. That process of hacking has been responsible, particularly over the past decade, for alerting the public and security professionals to major security flaws in software. What hackers see as a public service, pointing out dangerous and troubling

security risks, many people see as criminal activity. Many public releases of security holes came as a result of companies refusing to fix (or even acknowledge) security flaws in their products because *there is no regulation for security in software, and most important, there is no liability for software companies when their products create risks for consumers.* At one level, the work that hackers do is not entirely unlike the work of a watchdog organization or *Consumer Reports.* Admittedly, the outlook, style and demeanor are different, but the end results are the same. Hackers force computer software manufacturers to pay attention to security. They find security flaws, and when they point them out, we tend to associate hackers with the flaws, rather than placing responsibility with the corporations that write and sell bad software. We need to be careful to focus on the causes of such vulnerabilities and to not blame the messengers.

When facing a question as weighty as cyberterrorism, a very serious problem that you face is getting the facts. Almost everyone that you talk to has an investment in inflating the risks and the dangers that hackers pose. Everyone, hackers included, are invested in telling you that the threat is much worse that it is. Cyberterrorism is a term that is bandied about with increasing frequency, but it is also one that has almost no meaning. I have yet to hear anyone articulate a realistic scenario in which computer hackers would be able to effect significant economic or physical damage in order to be considered a "terrorist" threat. It is easy to imagine scenarios that sound like terrorism: For example, hacking into air traffic control and crashing planes, or hacking into the New York Stock Exchange and undermining the Stock Market. These things make great Hollywood plots, but there is no evidence that any such scenario is possible, much less likely. In fact, most of the research I am familiar with in this topic concludes just the opposite.

Cyberterrorism is a lot more difficult than many people assume. Because a power plant has a website, for example, does not mean that one could access controls for that power plant online. In most cases, in order to control the operation of a power plant, you must be *physically* inside the power plant. You would need to enter the building and sit down at a computer terminal. Such power plants are not controlled or accessible through the Internet or dial up modems. One cannot "hack" that power plant and shut it down. It is technologically, physically, and in every other way *impossible*. Systems that are well designed should all have similar access barriers, such as independent, non-public networks, physical barriers and sophisticated authentication and encryption schemes. Such access barriers make it extremely difficult to even reach places where damage might occur and will protect our most critical information infrastructure assets.

Furthermore, even if you were to assume that a hacker had the ability to hack into one of our nation's critical infrastructure assets, he or she would also need expertise in some other area, such as power plant management, air traffic control, or banking. Absent the expertise to effect some significant and targeted attack, even access to these systems would be of limited threat potential.

Also, most of our critical infrastructures are monitored and require human control to function. People tend to notice when things look suspicious. We may feel as though computers have come to control every aspect of our lives, but the reality is that humans still exert primary control over all the most important aspects. For example, if you looked at your schedule for the day and saw the entry "12:30: Jump off a bridge," you are not likely to follow that instruction, even if it is in your Palm Pilot or Outlook calendar. On the face of it, there is something wrong with that information and you become suspicious.

For the foreseeable future, acts of cyberterrorism, such as the ones usually imagined, will be very difficult to perform, unreliable in their impact, and easy to respond to in relatively short periods of time. In point of fact, there has never been an act of cyberterrorism committed, nor has there ever been, to my knowledge, a computer hacking incident that has resulted in the loss of life.

When these scenarios are proffered, I urge you to ask the tough questions about them. What additional security measures would have to fail for such an attack to take place? Scenarios that begin with the phrase, "First, a hacker breaks into an air traffic control center . . ." cannot serve as the basis for policy decisions about terrorism any more than "First, someone steals all the gold out of Fort Knox . . ." can serve as the basis for regulating decisions about banking. Before acting on these sorts of threats, we must be certain that these threats are grounded in some sense of reality. Take, for instance, the most frequently cited example of interference with air traffic control. Air traffic control systems are not readily accessible and, more to the point, they don't actually control anything. They provide radar data to controllers who use radios to direct pilots. Even if a terrorist were able to get access and cause

interference the human control measures, air traffic controllers monitoring the flights, and pilots flying the planes, on board radar, etc. would detect and correct for problems immediately. In practice, such an attack would be exceedingly difficult to carry out, if not because of access difficulties, because of the human control elements which provide an additional layer of security that is difficult to circumvent. By extension, then *every critical system should have safeguards in place, so that if something suspicious happens, it can be monitored and corrected.*

It is imperative, in turn, to understand security as a multi-layered process. How specifically would such an attack happen? This is the single most important consideration. Idle speculation is easy. Detailing the plan for such an attack is much more challenging. Do not assume that anything of vital importance is connected to the Internet. Just because a system is "networked" does not make it accessible through the Internet or even accessible from the outside at all. What kind of access would be required to cause such a catastrophe? I assure you, the threat is not a 16-year-old, with a Dell laptop hacking from his bedroom. In most cases, you will find that an attack would require someone to physically invade a space and get control without anyone noticing as well as requiring a detailed knowledge of the location and organization being attacked. *Therefore, our focus, through projects such as that National Infrastructure Protection Center, should be on controlling, regulating, and safeguarding access to these points. There is no substitute for a well designed system that controls access to critical systems.*

One of the great challenges you face is getting accurate, reliable information, both with respect to hackers and with respect to the computer and security systems that may be targets for attack. Hackers tend to exaggerate their own abilities out of a sense of bravado. And while there are hackers who can do damage to systems, disrupt e-commerce, or even force web sites offline, the vast majority of them can't. The ones who can, generally, don't.

Hacking stories make good copy, but they are very rarely accurate, tending to exaggerate threats and downplay the realities of the event. There is a big difference between hacking into NASA's central control system (which has *not* happened) and hacking into the server that hosts their web page (which has happened repeatedly). Most media reports fail to distinguish between the two (or to explain that hacking a web page is essentially the same as spray painting a billboard, posing very little actual risk). The media, moreover, tends to exaggerate threats, particularly by reasoning from false analogies such as the following: "If a 16 year old could do this, then what could a well funded terrorist group do?" The reality is that there is very little that a well-funded terrorist group could do that a 16-year-old hacker couldn't. And neither of them threatens us in a way that can rightly be called "terrorism."

Law enforcement, security consultants, and even software corporations are all highly motivated to embrace similar outlooks. It is to their advantage to have you believe that the threat to our nation's security is severe. Almost no one has any investment in a more balanced, nuanced, and complete perspective. It is that perspective that I hope you will seek out as you work to assess vulnerabilities and identify solutions.

My last comment has to do with what we might think of as a worst case scenario. Should an extremely talented hacker, who violates the ethic of hacking, manage to get access to a critical system, bypass all security measures, and launch an attack unnoticed by those monitoring the situation, it should be noted that this country has some of the best resources available to it to deal with, diffuse and neutralize such a threat. The faculty and students at places like MIT, UC Berkeley, Stanford, Purdue and Carnegie Mellon as well as organizations such as CERT and the National Computer Security Association provide our best defense against such threats. But these groups only provide that advantage as long as the network is open and accessible. *Security only gets better through testing, design, and redesign. The real threat to security is closing off avenues of exploration and examination. The more we know about our networks, the better we are able to defend them.* The more we know about the network's flaws, the better able we are to redesign it to eliminate these flaws. Testing our networks, probing them and finding those flaws is the only way in which we can be sure that they remain safe and secure and maintaining their openness is the only way to assure that if the worst does happen, that we can respond immediately, directly, and effectively.

Mr. HORN. The next presenter is Timothy G. Belcher, the chief technology officer of Riptech, Inc.

Mr. Belcher.

STATEMENT OF TIMOTHY G. BELCHER, CHIEF TECHNOLOGY OFFICER, RIPTECH, INC.

Mr. BELCHER. Chairman Horn and distinguished members of this committee, thank you for inviting me to provide my thoughts on the issues of cyberterrorism and critical information protection. I have already provided you with written testimony, and I would like to take a few minutes to outline some key points and issues.

First let me say that the networks that comprise our critical infrastructure are undoubtedly at significant risk of cyber-attack and compromise. The nature of these networks ensure that security is never going to be an absolute, but the vulnerabilities will always exist. The level of threat is increasing and, in my opinion, will continue to do so. The nature, complexity, and motivation of attacks against these networks have become and will continue to become more sophisticated over time.

I am the chief technology officer of a computer security company called Riptech. We perform two services that would be of interest to this committee in terms of experience. We assess client organizational networks for vulnerabilities; in effect, sometimes can become a hired hacker to test their defenses. Second, we provide a monitoring service that provides 24x7 monitoring of client networks, detecting and analyzing attacks for effectiveness and severity.

First let me talk about our assessment work. We have done assessments on over 50 critical infrastructure networks. Consistently, we have been able to demonstrate the viability of compromise to the most critical components of those networks. Those would include connectivity to the most critical components of power and energy companies, such as SCADA and EMS networks, financial transaction networks, and the inner workings of some of our government networks. Those organizations consistently had defenses in place, firewalls, intrusion detection systems, and our detections consistently went, by and large, undetected.

Second let me talk about our monitoring service and some of the information that is providing today. We are providing monitoring services for over 500 organizations, or approximately 500 organizations throughout the world. Our monitoring service is producing real dividends in terms of quantifiable numbers of the attacks these organizations are facing. All organizations are suffering some level of compromise in their attacks, some significant volume of increases in the attacks on them. Most notably, power and energy companies and financial services appear to be the most targeted sectors. Critical infrastructure companies represent nearly 20 percent of our clientele and are our fastest growing segment.

With regard to power and energy companies in our client base, 70 percent suffered at least some level of compromise over the last 6 months, up from 57 percent in the prior 6 months.

Again, these companies not only have defenses in place and have invested in technologies, but have also invested in obtaining an outsourced expert service to analyze the attacks against their organizations. They are still suffering. Most importantly, we have been

able to quantify a reduction in the success rates against these organizations over time, given proper defense.

Let me sum up by simply saying that critical infrastructure is at significant risk; and, in order to achieve any successful and acceptable level of defense, they must establish reliable detection and response mechanisms which are unavailable today.

Thank you for your attention, and I look forward to any questions that you may have.

Mr. HORN. Thank you, Mr. Belcher.

[The prepared statement of Mr. Belcher follows:]

STATEMENT OF
TIMOTHY G. BELCHER
CHIEF TECHNOLOGY OFFICER, RIPTECH, INC.
BEFORE THE
U.S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

Chairman Horn and distinguished members of the committee, thank you for inviting me to provide my thoughts about the issues of "Cyber Terrorism and Critical Infrastructure Protection". I am hopeful that my remarks, written testimony, and the answers I provide to your questions will provide you with a greater understanding of several issues of critical importance to our nation's information security posture.

My name is Timothy G. Belcher, and I am the Chief Technology Officer and co-founder of Riptech, Inc. Located in Alexandria, VA, Riptech offers a range of information security services to hundreds of companies both in the United States and in over 40 countries worldwide. Given that all of the co-founders of Riptech have served in the United States armed services, our company has always maintained a particular interest in the information security posture of the government and our national critical infrastructures. Additionally, "critical infrastructure"[1] companies constitute a substantial portion of Riptech's client base, and therefore represent a particular interest at our company.

The first goal of my testimony is to explain how and why significant vulnerabilities exist in most information networks that support critical infrastructures. As evidence of this challenge, during the course of conducting more than 50 vulnerability assessments on behalf of critical infrastructure companies, Riptech demonstrated the possibility of network intrusions at every company. I will highlight some of the most common vulnerabilities that Riptech detected during these experiences, as well as a few of the possible scenarios that could possibly occur as a result.

My second goal is to provide you with some guidance about the threat of cyber attacks specifically targeted at critical infrastructure companies. These observations are based on Riptech's experience monitoring the network security for hundreds of corporate networks. As a result of this monitoring activity, Riptech produces periodic reports that summarize attack activity observed against its entire client base. These reports have generated several interesting insights about the nature of cyber attack activity targeted at certain critical infrastructure industries. Although these observations are based only on attacks detected against Riptech clients, I believe they can provide the members of this committee with valuable information about the overall nature of the threat.

Lastly, I will share with you with some specific concerns that I have about two particular critical infrastructure segments: financial services and power and energy. My experience

[1] As outlined in Presidential Decision Directive 63 (PDD-63)

with the information security challenges in both of these industries has provided me with a deeper understanding of the unique vulnerabilities that they face.

VULNERABILITIES

Before the Internet became a common component of normal business operations, many of the crucial information networks at financial services, power and energy, and telecommunications companies were both logically and physically isolated from other components of a corporate network. As a result, the security threat to these systems was minimized because attackers could find few points of access to this portion of the network. Over time, however, competitive pressures, technology advancements, the need to develop economic efficiencies and, in some instances, deregulation forced many of these companies to embrace Internet protocol (IP) based technologies to help manage their corporate and operational information. While this drive to "link" all components of a company's network together under one protocol has enabled these businesses to operate more efficiently, it has also increased the risk of compromise as well as the diversity of information at risk.

From a security standpoint, allowing easier access to operational, customer, and supplier information, combined with the expansion of corporate IT boundaries, vastly increases the number of network vulnerabilities. As information system advancement escalated over the past decade, information security vulnerabilities have shown a corresponding increase. Simultaneously, the number of network access points has increased as personnel both inside and outside of the company gain a higher level of access to crucial business information and networks. As a result of these developments, Riptech frequently detects a wide variety of vulnerabilities that impact networks at critical infrastructure companies; a few of the more common of these vulnerabilities are:

1. **Excessive Employee Access.** Company personnel often have permission to access a wide variety of sensitive corporate and operational information resources via e-mail and other business applications. This level of access often extends beyond what is actually necessary. Attackers who have compromised an employee workstation can then use this access to their advantage and further penetrate the corporate network.

2. **Excessive "trust" of third parties.** Externally, most contemporary corporate network configurations provide numerous (and often unrestricted) points of access to outsiders such as contractors, consultants, vendors, suppliers, and customers.

3. **Poor network configuration.** Architecture problems that deviate from the classic gateway security model often exist on networks. Examples include the use of utilities that provide direct access to internal networks.

4. **Inadequate password protection.** Although access to many of the networks and systems of critical infrastructure companies require passwords, these passwords

are often extremely simple and, in some cases, exist in the default mode. Additionally, network administrators often use identical passwords for a number of different systems.

5. **Unintended "dial-up" and/or wireless access.** Access to corporate or internal networks is commonly gained through the use of dial-up modems or wireless networks. Such access can allow an attacker to bypass security technologies, such as firewalls, and gain direct access to the internal network.

6. **Improper network segmentation.** A common practice at many critical infrastructure companies is the establishment of separate networks that operate the critical infrastructures (i.e. SCADA systems[2]). Although these systems are, in theory, isolated from corporate networks and the Internet, many companies have not properly segmented these networks with firewalls and intrusion detection systems.

As a result of these vulnerabilities, critical infrastructure companies must be concerned with more than simple web site security. They also must be wary of the possibility of attackers gaining access to and, in some cases, damaging key operational systems that conduct financial transactions, control power grids, or any number of other critical infrastructure operations. It should also be noted that these companies are often inundated with the daily rigor of security management and monitoring such as updating security patches, monitoring network access, and analyzing firewall logs. The demands of information security cause even the companies with top security programs in place to experience a security incident due to some type of oversight or unknown vulnerability.

Does this mean it is impossible for these companies to completely protect themselves from "cyber" attacks? Probably. Although security managers still have powerful tools, such as best practices configuration management, access code and password protection, and firewalls, security is never an absolute. In sum, the challenges facing security managers have grown in number and complexity, and keeping up with these challenges is now more about managing risk than providing complete protection.

THREATS

As I mentioned earlier, Riptech monitors the security of many critical infrastructure companies on a 24x7 basis. Drawing from the aggregation of data that we collect about our client base, Riptech produces a series of semi-annual Internet Security Threat Reports that provide a broad quantitative analysis of Internet-based attacks targeted at hundreds of organizations during the preceding six-month period. We believe this report provides a unique view of the state of Internet attack activity.

Perhaps the most important finding from the report is that, although attack volume varies, cyber attack activity has steadily increased over the past 12 months. During the first six months of 2002, for example, attacks increased by 28% over the preceding six-month

[2] Supervisory Control and Data Acquisition

period. When analyzed on a per company basis, this means that the average company faced 32 attacks per week between January and July of 2002, as opposed to 25 attacks per week between July and December 2001.

Additionally, some of the key findings that were identified in the most recent report concerned the number and source of attacks against key critical infrastructure industry sectors. For example, Power and Energy, and Financial Services companies experienced the highest rate of overall attack activity, and also suffered relatively higher rates of severe and highly aggressive attacks during the past six months. Specifically with regard to power and energy companies, 70% suffered at least one severe attack during the first six months of 2002, as opposed to 57% during the last six months of 2001.

One additional point of concern that was highlighted in the report involves the relative frequency of targeted attacks. Targeted attacks are those where Riptech noted that the attack was not part of a larger sweep or scan of a number of networks, but rather appeared to be focused on one network in particular. Although conventional wisdom, and even my own thoughts, have tended to place the number of targeted attacks at about 10-15% of all attacks, our findings indicate this number is closer to 40%. This suggests that many companies targeted by attackers are being attacked for a particular purpose.

In sum, I think it is clear that critical infrastructure companies are experiencing a high rate of attacks from sources that may be targeting them for a particular reason. Although I would hesitate to speculate about the intentions of such attackers, I think the fact that these networks are the focus of so much activity is in and of itself a major cause for concern. When combined with the number of vulnerabilities that I have already highlighted as a part of this testimony, it is clear to me that critical infrastructure companies need to be more diligent in protecting their networks.

CRITICAL INFRASTRUCTURE INDUSTRY OBSERVATIONS

Although it is difficult to determine the most likely result of a cyber attack on a critical infrastructure company, it is important to be aware of the potential outcomes. I have already explained that companies from two industries, financial service and power and energy, appear to be experiencing a greater number of attacks than the average company. Now I would like to explain a bit more about the attacks that present the greatest risk to these industries.

It has long been believed in the information security community that financial services institutions, particularly banks, are among the most secure companies in the world. It is often assumed that companies in this industry maintain the most mature information security programs. Further, because it is common for financial services companies to link security spending directly to profit risk figures, many of the largest financial services companies have made large investments in the most effective security technologies to protect their assets. Unfortunately, as with many industries, the smaller financial services companies lack the same resources to protect their infrastructure. As a result, many networks for companies of this type are easily compromised. Additionally, many small

banks and credit unions do not maintain diligent and consistent risk management programs, and are thus less prepared when an intrusion occurs.

Among the major concerns that financial services institutions need to be aware of in the event of an intrusion are:

- **Direct Financial Loss.** Network attacks on financial institutions are becoming more common each year. Many times these attacks go undetected until after substantial damage occurs. This danger is of particular interest for financial services companies where the target of cyber attacks is likely to be the systems that control financial transactions.

- **Legal Implications.** An appropriate and current information security posture is, in my opinion, the best type of 'due diligence' a company can provide in order to minimize the risk of civil lawsuits.

- **Damaged Reputation.** Financial institutions store a wealth of confidential customer and corporate data that, if released, could have a devastating impact on public perception. Publicized information security breaches at financial institutions could significantly damage a financial institution's ability to attract and maintain customers.

I leave it to this committee to consider the broader implications that an intrusion at one or more financial services institution can have on the overall critical infrastructure. However, I think it is important to understand the great amount of emphasis that is placed on both privacy and security by the public with regards to financial data, as has already been addressed by legislation, such as the Gramm-Leach-Bliley Act.

Power and Energy companies are also an important component of critical infrastructure protection that should be addressed. Although these companies are rapidly developing a greater awareness of the security challenges that they face, many are still a long way from establishing adequate isolation of critical network components while still meeting the demand for network access brought on by the forces of deregulation and increased business competition. As with the financial services industry, the largest of these companies have often implemented sophisticated security architectures to address their vulnerabilities, but the industry as a whole faces considerable challenges.

Perhaps the most common and most concerning threat to these companies is the misconception among many managers at power and energy companies that operational networks (often called SCADA networks[3]) are isolated from their own corporate networks and the Internet. As these systems are used to control the power grid and, therefore, are often the most directly related to critical infrastructure protection, I think it is important to understand the major misconceptions that Riptech has identified about the security of SCADA systems.

- **MISCONCEPTION #1** – *"The SCADA system resides on a physically separate, stand-alone network."*
  Current networking and administration concepts have actually forced a large number of open connections. Once a corporate network is breached through the Internet, a company's control networks are also exposed.

- **MISCONCEPTION #2** – *"Connections between SCADA systems and other corporate networks are protected by strong access controls."*
  From the experience of Riptech vulnerability assessments, the controls in place often allow access to the SCADA network from the corporate network, even through a firewall or other guard.

- **MISCONCEPTION #3** – *"SCADA systems require specialized knowledge, making them difficult for network intruders to access and control."*
  Although it may require years of experience to appropriately control power flow, an attacker can learn to disrupt these systems in considerably less time. Unfortunately, this threat is compounded by the fact that much of the information outlining the inner workings of SCADA systems can be obtained from public sources.

CONCLUSION

Once again, Congressman Horn and members of the Committee, I thank you for inviting me to participate on this panel. I believe that, although critical infrastructure companies face very real threats, there is certainly hope that appropriate and effective practices may be established in the future. While I believe that we have relied too much on luck in the past to protect us from a truly catastrophic incident involving cyber-intrusions, I believe that critical infrastructure companies have the ability to create adequate protections from a majority of the dangers they presently face. When provided with the right tools and incentives to protect their networks from all levels of threat, a significant portion of the vulnerabilities can be addressed and avoided completely. I remind you, however, that security is not an absolute, and that threats and vulnerabilities will always be with us. A significant amount of risk to these infrastructures already exists, and it will take work from both government and the private sector to bring information security to the level that is necessary.

Thank you for your attention during my remarks, and I look forward to answering any questions you may have at this time.

Mr. HORN. Our next presenter is Alan Paller, director of research at the SANS Institute.

STATEMENT OF ALAN PALLER, DIRECTOR OF RESEARCH, SANS INSTITUTE

Mr. PALLER. Before I start my remarks, I want to bring greetings from Bob Chartrand, first, and also tell you that model that you provided to this body, this model of action, the model of taking on unpopular causes, what you did in——

Mr. HORN. Move the mic up. It's very important, what you are saying.

Mr. PALLER. You really have set a model, and I hope that model will follow you. And you are going to be sorely missed around here. One of the actions that I am going to talk about today is something that doesn't take more than 6 months; meaning, if you want to have something similar to the impact on security that you had on Y2k, I think you actually have it in your—it would be tough, but you have it in your hands to do it. So, let me go on.

We train the people who are the frontline soldiers in security. We have 30,000 of them who have attended SANS training and go out and try to protect the computers. So we have to clean up after the messes. And right now, as we speak, the problem is getting worse. And the reason the problem is getting worse is that as all of us are sitting here, approximately 7,000, maybe 10,000 new computers will be installed and connected to the Internet, and almost every one of those will be installed with known vulnerabilities. That means almost every one of the machines being sold while we are sitting here is going to come in with known vulnerabilities. And between 2- and 3,000 computer programs are active on the Internet at all times—not people—programs, searching out every new address to see if they can take over those machines, put a Trojan in there, and be ready for an attack later. That is happening while we are sitting there.

I am happy to be on the first panel, because I think if we define the problem right, then the actions we take might actually help solve the problem. And so I would like to give you the four reasons that I think cause that set of problems to exist and the two actions I think you could take that would help solve them.

One is that the vendors actually deliver software that has known vulnerabilities. The people who install it trust the vendor, so they install it exactly the way the installation technique tells them. And, because they are so busy, they don't change that. So, most of those machines that are being installed unsafely today will still be unsafe in 90 days and still be unsafe in 180 days.

Second—and two of these next three are going to be counterintuitive. The risk-based approach that many people say is so good, actually is causing part of the problem. While people are doing risk analysis and writing reports, all these new machines are getting installed. And, worse, they say "Let's just fix the ones that are the highest risk." But since all the machines are connected together, if Tim had given you his demonstration of how you actually break into a utility company, he would have used the fact that one of the machines that had been installed that nobody cared about, was weak, to jump off into the other machines.

So if we are going to solve the problem, we have to start by stopping the machines from being vulnerable on the day we install them.

The third cause is that the government—we talk about critical infrastructure as if it is industry. The government is a part of the critical infrastructure. We care about government, and government is doing a not-very-good job of being a model for the rest of the critical infrastructure. And it turns out in this arena, because technology is transferrable so quickly and techniques are transferrable so quickly, it turns out that here, if the government actually did some good, the problem could roll over very quickly.

And I think Dick Clarke's announcement last week of benchmarks is an example of how that can happen almost instantaneously. But the government hasn't been a great model, and that has to change quickly if we are going to ask industry to change. How can you ask a CEO to "believe me and trust me" and say to you, "I'm going to do what you need to help protect the infrastructure, when you don't do what you need to help the infrastructure?" It is really hard for a CEO to take you seriously.

And the last one I think is the most counterintuitive. And that's that most of the money being spent by Government on cyber-security is being wasted, and the money has gone up radically in the next—in the last 2 years—at least an order of magnitude. Think of that money as having a huge vacuum cleaner sucking it out, and that the vacuum cleaner is people who like to write reports, and they are taking the money and they are writing reports. And the problem is, none of the money is left for the people who actually have to secure the systems. So you get all that security money out there spent on the studies about why you are so bad and it is so easy to find fault. And it doesn't take as much skill level to find fault than it does to fix it. It is much easier to—you can come out of grade school and run one of these penetration testing tools and do a pretty good job of delivering the report because the vendors make it pretty, but the difficulty is there's nobody there to fix it. So you have got $1 billion telling people what to do and nothing left fixing it.

OK, two actions and then I'll quit.

Action one—and this is the report card that you are the father of. Action one is that there are benchmarks, there's several of them. And NASA is the one actually that's proven this works. This is not a new idea. NASA has actually demonstrated beyond a doubt that this approach works. You take a set of vulnerabilities that matter, and you systemically make sure every single computer in your entire NASA facility all across the whole country doesn't have them anymore. And they took the vulnerabilities down by 93 percent and they took the number of successful attacks down radically, even though the number of attempted attacks is up radically.

Dave Nelson, who is the deputy CIO, can give you the hard data on this. But this works. And if you—if you just take what they did and apply it to the rest of government over the next 6 months, we could fix somewhere out in the 70th to 80th percentile of the vulnerable machines real quickly.

The second idea is a little harder. All these consultants that are spending money on vulnerability testing ought to be asked—and

you are the only guy I can think of who could make this happen, because OMB doesn't seem to be awake to this. All these people who are doing vulnerability tests aren't staying to fix the problem. And if they are so smart that they can tell you what you are doing wrong, why aren't they staying to make sure the problem disappears? So solution 2 is some way of getting an amelioration phase into these consulting contracts so that the people actually have to fix it, they can't just send you a pretty, colorful report and tell you how bad you are and then go on to the next guy, would be very helpful. Thank you.

Mr. HORN. Thank you. You have given us numerous months. We can take care of your ideas.

[The prepared statement of Mr. Paller follows:]

Testimony of Alan Paller
Director of Research, The SANS Institute

Before the
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS
United States House of Representatives
Hearing on
"Cyber-terrorism: Is the Nation's Critical Infrastructure Adequately Protected?"
July 24, 2002

Introduction

Chairman Horn, Ms. Schakowsky and Members of the Subcommittee, thank you for inviting me to testify today on what the government can do to help protect the critical infrastructure. I am deeply honored. My name is Alan Paller. I am Director of Research for the SANS Institute. SANS is the primary training organization for the technologists who battle every day to protect the computer systems and networks in the global infrastructure. SANS alumni, more than 29,000 in all, are the intrusion detection analysts, security managers, security auditors, firewall analysts, system and network administrators, incident handlers, forensic analysts, and law enforcement officers who are responsible for building, maintaining, and auditing their organizations' cyber defenses, fending off attackers, and, when attackers succeed, investigating the crime and tracking down the criminals. In addition to providing formal education and training, SANS also is a source of continuing education to these technologists on the front-line of protecting our critical infrastructure. Each week, more than one hundred and fifty thousand individuals receive SANS *NewsBites* and SANS *Security Alert Consensus* to keep them up to date on new developments in information security and new threats. In addition, we operate the Internet early warning system, Internet Storm Center, as a public service. Storm Center provided the early warnings for both the Lion and Leaves worms and provided much of the data on the rate of spreading of Code Red.

Our students are the front-line warriors in a constant fight against cybercrime. Every day, they are forced to engage the criminals who seek to use the Internet for financial gain or to disrupt commerce and government. The prize to the winners is control of the systems that operate our economy and provide the essential services on which we all depend.

I have had the great pleasure of working closely with most of the other people testifying today and in most ways their views and my views as SANS director are similar. Instead of repeating what they will say, I hope to illuminate four characteristics of the problem faced by cyber defenders that you may not hear from the other witnesses, and what each means to the federal initiatives to assist the private sector in protecting the infrastructure.

A well planned campaign to solve these problems will be a huge step toward stemming the tide of cyber attacks, and your Subcommittee is in a unique position to make a difference.

I'll list the four challenges first and then suggest two actions the government can take, with your leadership, to meet these challenges.

1. **Off the shelf software has caused and continues to cause critical security problems. Many software installation routines configure new software so that it is immediately vulnerable to exploitation.** In other words it is installed with known vulnerabilities. MIT measures the amount of time after a new system is connected to the Internet before that same system is probed by an attack program looking for a vulnerable system to take over. The average last year was under 300 seconds. The number of automated attack programs on the Internet is growing, so those 300 seconds are probably shrinking. Five minutes is not enough time to download patches and correct other configuration weaknesses. If the system is not configured safely before it is connected to the Internet, it is at enormous risk.

   Software vendors cause this problem partly because of their manufacturing and distribution process and partly because of their desire to make systems easy for their users. Their manufacturing and distribution process requires them to make CDs months before the client purchases and installs the CD. Any vulnerability found in the software in the intervening months will be installed on the client's computer. In addition, the software vendors turn on many services the users do not need and do not know they have – services that may later be found to be vulnerable.

   There is new proof that these vulnerabilities are caused by the default installations. Research completed over the past few weeks compared vulnerabilities found in systems installed using the default installation and systems installed using the new security benchmarks announced by the White House and GSA and NIST and the Center for Internet Security last week. The result was that the number of vulnerabilities is reduced by 80 to 88% simply by using the minimum configuration benchmarks. It would be foolhardy to install software without the benchmarks, yet, prior to the announcement, nearly every organization still did.

   Jim Purdy showed you, in his testimony, how electrical utility control systems can be breached. The first and most critical step in his demonstration attack would almost certainly been blocked had the server been set up with a minimum security configuration.

   Similar configuration problems also impact the specialized systems at telecommunications companies and other elements of the critical infrastructure.

2. **Too much emphasis on a risk-based approach leads to many important systems being left unsecured.** When laws and auditors demand that organizations perform risk assessments before making substantial investments in security, some organizations take the requirement too literally. While they are undertaking risk

assessments, they continue running hundreds or thousands of systems, they continue installing new systems, and they continue having contractors manage and acquire systems, just as they are – without any substantive security configuration improvements. Yet we know that most systems installed without special security configurations are vulnerable to common attacks. The end result is that hundreds of thousands of systems remain vulnerable and many thousand are exploited.

Even when a vulnerability test or penetration test is done, the problem is not solved. The test generally checks only a small subset of potentially vulnerable systems. After the test, the organization may fix the items found in the test, but they nearly always leave in place all the vulnerabilities in all the other systems that were not checked.

Many organizations also misinterpret a risk assessment edict to mean that systems that have no important data do not deserve security attention. But hackers don't go after the critical systems directly. They attack unprotected systems at the target site and then use those systems as inside platforms to attack the critical systems. And automated attack programs can and usually do try to attack every system you deploy.

Since all the systems are connected, weak security on any system puts all the systems at risk. That means that the work that needed to secure a critical military system and the work needed to secure a seemingly unimportant web server overlaps by 60 to 80%. There are extra things that are needed for military and nuclear power plant systems, but there are many steps that must be taken regardless of how the system is being used. Too often a risk-assessment-first mentality delays the necessary security work on many systems. Sometimes those systems are never secured.

3. **The federal government has not led by example either in sharing information or in securing its own systems.** How can we expect CEOs of critical infrastructure companies to take the government seriously when government agencies are constantly held up to ridicule because of their weak security? Last week alone, an Army Research Laboratory web site was hacked and the GAO issued another report showing how badly a federal agency manages security on its systems. That type of coverage shapes how CEOs judge the seriousness of the federal commitment to cyber security.

4. **The vast majority of the money spent by the federal government on security doesn't actually improve security.** Firewalls help improve security, but many of the other rapidly growing expenditures for security have indirect impacts. Penetration tests, red teams, vulnerability tests, risk assessments cost hundreds of millions of dollars. That money buys reports containing recommendations or new policies. And the reports are usually sent to the operations people who actually have to implement the recommendations and new policies. But very little of the budget for security has gone to provide the operations staff with additional system administration talent to implement all those recommendations. Without extra staff, they cannot implement the

recommendations and the money spent to make the recommendations is wasted.

This subcommittee has a unique opportunity to make a significant difference in all four of these areas by taking two actions.

Action 1: Require, as part of the GISRA/FISMA bill, that each agency measure the security configuration of every system they and their contractors deploy to see how closely the systems meet minimum security configuration benchmarks, and report the results for each sub-agency and the agency as a whole. NASA has already done this. Under the leadership of Dave Nelson, the Deputy CIO there, NASA has radically reduced the number of successful attacks and the amount of damage that is being done by cyber attacks, despite an equally radical increase in the overall number of unsuccessful attacks NASA computers faced. In a White House meeting last December, Dave told an assembly of Inspectors General, CIOs, NSC and OMB staff, and one Congressional staffer that the entire cost of the program was less than 3 percent of his $110 million security budget. Here's a program that works and is relatively inexpensive. Agencies can use NASA's benchmarks or those announced this week by Richard Clarke and the Center for Internet Security, or any others that they can show to be effective. If security configurations do not get measured, they won't get fixed. A report card makes measurement work. This single change to GISRA/FISMA will make federal systems much, much safer, and make the government a model for others to follow.

Action 2. Require that penetration testing projects include a vulnerability amelioration phase. It's too easy to find fault. If a testing team reports finding a vulnerability, the team ought to know enough about how to remove the vulnerability to help the agency do it quickly, safely, and inexpensively. Otherwise what's the use of spending the money on the penetration test or vulnerability assessment?

These two actions will play a huge role in meeting all four of the challenges I outlined earlier. (1) Shortly after agencies start measuring systems against secure configuration benchmarks, vendors will begin delivering software that automatically configures itself according to the benchmarks. (2) These configuration standards will eliminate the problems caused by over emphasis on risk-analysis because safely-configured systems will be protected from the basic threats that apply to all internet-connected systems. This government initiative demonstrates that the federal government is serious about protecting its own systems and provides a model that companies can emulate. Once they learn of the rapid decreases in vulnerabilities of federal systems, commercial organizations will see the value in using the same benchmarks or adapting them for their special needs. (4) When most federal systems are pre-configured to avoid common attacks, penetration testing and vulnerability scans will be much more likely to find new problems and the testers will be able to help the agencies fix those problems immediately.

Clearly there are other important steps that can be taken to improve security, but I submit that no other actions involving Federal IT programs will do as much to turn the tide against cyber attacks.

We at the SANS Institute and, I believe, the entire community of SANS alumni, will continue to work every day to do our part to help reduce the threat.

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

Mr. HORN. We now go to Scott Charney, the chief security strategist of the Microsoft Corp. Mr. Charney.

STATEMENT OF SCOTT CHARNEY, CHIEF SECURITY STRATEGIST, MICROSOFT CORP.

Mr. CHARNEY. Mr. Chairman, thank you for the opportunity to appear today at this important hearing on cyberterrorism and critical infrastructure protection. My name is Scott Charney, and since April 1st, I've been Microsoft's Chief Security Strategist.

Microsoft works with industry leaders and governments around the world to identify threats to computer networks, share best practices regarding computer security, and prevent computer attacks. While we have worked diligently on cyber-security for several years, this effort accelerated after September 11th, and was crystallized for Microsoft when Bill Gates launched our Trustworthy Computing initiative in January.

Today I would like to address IT security issues broadly, and then use the Trustworthy Computing initiative as an example of how one company can take steps, both on its own and with others in industry and government, to address cyber-security. And finally, I will propose several things that Congress can do to address cyber-attacks.

By way of background, prior to joining Microsoft I served as the Chief of the Computer Crime and Intellectual Property Section at the Department of Justice where I helped prosecute nearly every major hacker case in the United States, and international hacking cases as well, from 1991 to 1999. Based on those experiences, Mr. Chairman, I know two things with certainty:

First, operating systems software is one of the most complex things we have ever built, and it may always have vulnerabilities.

Second, society has always grappled with a criminal element, and this criminal element can be smart and malicious and will seek ways to exploit vulnerabilities in software. As a result, it is impossible to completely prevent cyber-attacks, and it places the IT industry in a perpetual race against cyber-criminals to maintain Internet security.

We take our cyber-security responsibility very seriously, and perhaps most importantly, Bill Gates spearheads our Trustworthy Computing initiative. This is not a one-time event, but rather a change in the way we do business. It has four pillars: reliability, security, privacy, and business integrity. And those four pillars go to the heart of our culture and the way we create products and services.

Today I want to focus on the security pillar, where we are working to create products and services that I call S D3: secure by design; secure by default; and secure by deployment.

Secure-by-design centers on creating products that are inherently more secure. To do this, we recently provided advanced training for several thousand developers, and conducted extensive code reviews and threat modeling. In fact, we stopped Windows development for over 2 months to do that.

Secure-by-default entails shipping products to customers in a lockdown position. This means that customers must consciously de-

cide to enable features, leaving other unused services off, and thereby narrowing the attack surface of a production.

Secure-by-deployment focuses on making it easier for consumers and IT professionals to maintain systems. For example, any Windows XP user can be automatically notified when critical updates are available for download. In fact, as Allan Paller has noted, when people first deploy software, they may already be at risk because there is some time from development to market. But with this kind of technology, the minute you load the software, the first thing you may get is that little notification that a patch is ready to be deployed. So we are working hard to automate that process.

But we do not work alone in this effort. For example, the announcement last week of a baseline security configuration for Windows 2000 demonstrates the positive results that flow from a voluntary public/private partnership involving a broad range of organizations. Microsoft reviewed the proposed settings, and we expect that some Federal CIOs will incorporate these promptly.

This work stands besides our coordination with entities such as the Partnership for Critical Infrastructure Security, John Tritak's Critical Infrastructure Assurance Office, the National Cyber Security Alliance coordinated by Dick Clarke's White House Office of Cyberspace Security, the FBI's National Infrastructure Protection Center, and, of course the IT-ISAC, which we helped create.

There is also a strong roll for government in this area, and I would like to close by addressing some areas where more work can be done. As you consider creating the Department of Homeland Security, please know that we support the effort and we would like to see a strong cyber-security component in the new Department. Our support extends to language that facilitates cyber-security information sharing by granting an exemption from the Freedom of Information Act.

We also applaud the House for passing H.R. 3482, the Cyber Security Enhancement Act of 2002. We are pleased that this bill strengthens law enforcement's ability to deter cyber-crime by permitting the U.S. Sentencing Commission to grant Federal judges more flexibility in sentencing cyber-criminals.

There are other steps that Microsoft respectfully suggests the government take to help protect our critical infrastructures. First, we support the forfeiture of personal property such as computer equipment used in the commission of cyber-crime.

Second, we strongly support increased funding for law enforcement. These hardworking individuals, many of whom were former colleagues of mine when I was at the Justice Department, are chronically overworked, understaffed, undertrained, and underequipped.

Third, we support increased funding for cyber-security research and development, and we look to the government to lead by example in securing its own systems through the use of reasonable security practices, an issue that Allan has already touched on.

Fourth, we believe that greater cross-jurisdictional cooperation among law enforcement is needed for investigating cyber-attacks, since cyber-criminals may reside anywhere.

In conclusion, Microsoft pledges to remain a leader in industry efforts to secure products and services. Americans, their govern-

ment, and the critical infrastructures they depend on every day face growing cyber-security challenges. Working with our government partners and industry peers, we are committed to preempting, catching, and prosecuting cyber-criminals to protect the computing experiences of our customers and the cyber-security of our Nation.

Thank you.

Mr. HORN. Thank you. And we will have a lot to ask you about, with one more presenter.

[The prepared statement of Mr. Charney follows:]

Prepared Testimony of Scott Charney
Chief Security Strategist
Microsoft Corporation

Before the
Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations
Committee on Government Reform
U.S. House of Representatives

July 24, 2002

Mr. Chairman and Committee Members, thank you for the opportunity to appear today at this important hearing on cyber-terrorism and critical infrastructure protection.

My name is Scott Charney, and I am Microsoft's Chief Security Strategist. Microsoft works with industry leaders and governments around the world to identify security threats to computer networks, share best practices and prevent dangerous computer attacks. Like many other information-technology (IT) companies, we have seen security threats grow, and we are responding to prevent harm caused by those who simply launch scripts to potential cyber-terrorists. While we have worked diligently on cyber-security for several years, this effort accelerated after September 11th and was crystallized for Microsoft when Bill Gates launched our Trustworthy Computing initiative in January. More recently, he reported on our progress to date in an executive e-mail distributed on July 18, 2002.[1]

Today I would like to address IT security issues broadly, then use the Trustworthy Computing initiative as an example of how one company can take steps on its own and with partners to address cyber-security. And finally, I will propose several things the Congress can do to help prevent and manage cyber attacks and catch those who perpetrate them.

As Chief Security Strategist, I oversee the development of strategies to implement our long-term Trustworthy Computing initiative and create more secure products, services, and infrastructures. My goal is to reduce the number of successful computer attacks and to increase the confidence of all IT users. Not only do I work on Microsoft products and services, but I also collaborate with others in the computer industry and the Government to make computing more secure for all users.

Prior to joining Microsoft, I was a principal for the professional services organization PricewaterhouseCoopers (PwC), where I led the firm's Cybercrime Prevention and Response Practice. In that capacity, I provided proactive and reactive cybersecurity services to Fortune 500 companies and smaller enterprises. Before joining

[1] http://www.microsoft.com/mscorp/execmail/2002/07-18twc-print.asp.

PwC, I served as chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division of the U.S. Department of Justice where I helped prosecute nearly every major hacker case in the United States from 1991 to 1999. In that capacity, I also worked with Congress to enact the National Information Infrastructure Protection Act of 1996, and served on U.S. delegations to various international organizations working to harmonize government responses to cyber-crime.

I. Cyber Attacks And Critical Infrastructure Protection Are A National Challenge.

Mr. Chairman, the information technology revolution has transformed all aspects of our society. And this transformation will continue as computing technology is embedded in a wide range of devices and as those devices become increasingly networked. But our society's increasing dependence on computers means that the disruption of our networks – whether due to nation-states, terrorists, criminals, or simply pranksters – could seriously impair public safety, national security, economic prosperity and, more generally, our way of life. An attack against the information technology backbone of one of our nation's so-called "critical infrastructures" – such as communications services, energy, financial services, manufacturing, water, transportation, health care, and emergency services – could disrupt Americans' physical and economic well-being and have a worldwide impact. An attack against the U.S. that combines both cyber and physical elements could be particularly devastating, such as a physical attack against a building combined with disruption of the telecommunications infrastructure needed to provide emergency services to the physically affected area.

More specifically, cybercriminals could attack our computer systems in a variety of ways, causing serious consequences including: (1) compromising the integrity of data, such as deleting records of financial institutions; (2) breaching the confidentiality of data, such as obtaining information from nuclear power plants which can then be used to plan a physical attack; and (3) acting as "weapons of mass disruption" to take-down key Internet nodes whose failure would then lead to a "cascading" effect, meaning wide-ranging disruption of other parts of our critical infrastructures.

The President's recently-released *National Strategy for Homeland Security* states how a cyberattack against one critical infrastructure could have cascading effects against other critical infrastructure networks; for example, disrupting a water supply authority's digital controls over water distribution could lead to a shutdown in electrical generation facilities, which in turn could cause widespread blackouts or brownouts But we need not speculate, as we have already had a cyber attack that caused cascading effects. Several years ago, a juvenile in Massachusetts disabled a telephone switch and consequently disrupted air traffic control at a regional airport served by that switch.

The challenge of cybersecurity has been with us ever since the Internet grew beyond its original purpose as a military communications network. The *Morris Worm* disabled portions of the Internet as long ago as 1988. And several publicized examples of viruses and worms over the last few years are the latest tangible reminders both of the widespread damage that worms and viruses can cause and that no vendor's platform is immune. The *I LOVE YOU* virus of 2000 caused an estimated $8 billion in damages.

The *Ramen* and *Lion* worms attacked Linux software to deface websites and extract sensitive information such as passwords. The *Code Red* worm caused an estimated $2.4 billion in damages by exploiting Windows server software to deface websites, infect computers, and make computers susceptible to attack by third parties. The *Trinoo* attacks exploited vulnerabilities in the Solaris operating system to stage distributed denial of service attacks against several prominent websites, causing an estimated $1.2 billion in damage. Most importantly, perpetrators are seldom identified and prosecuted. For example, the *I LOVE YOU* virus writer was found but remains free since the laws of his country did not criminalize his actions.

Unfortunately, we know two things: First, operating system software is one of society's most complex creations, and thus it will always have vulnerabilities. And second, because smart, malicious individuals will always seek and exploit these vulnerabilities, it is impossible to completely prevent cyber attacks. This places the IT industry in a perpetual race against cyber-criminals to maintain the Internet's security.

Finally, U.S. critical infrastructures were and are designed, deployed and maintained primarily by the private sector. That is why this Administration and its predecessor have emphasized that securing critical infrastructures requires a partnership between Government and industry. Voluntary cooperation and industry-led initiatives, supported by appropriate Government cybersecurity initiatives, will work best to address computer security issues. As I will describe below, Microsoft is at the forefront of industry's efforts to work closely with the Government to secure our nation's information technology infrastructure.

II. Microsoft's Response To The Threat Of Cyber-Attacks Against Our Nation.

Microsoft is working with industry leaders and governments around the world to identify security threats to computer networks and share best practices, and this starts from the very top. Our senior leadership contributes its expertise to national policymaking on cyber-security and critical infrastructure protection, and from Bill Gates to each developer, we are devoting our resources and energies to our ongoing Trustworthy Computing initiative. We also engage on an operational level in assisting Government agencies to prevent and investigate cyber-attacks.

A. Microsoft's Senior Leadership Participates In National Policymaking To Strengthen Our Nation's Cybersecurity.

Our top officials are committed to strengthening our nation's cyber-security and are involved in national cyber-security policymaking. Craig Mundie, Microsoft's Senior Vice President and Chief Technical Officer for Advanced Strategies and Policy, was appointed by the President to the National Security Telecommunications Advisory Council (NSTAC). The NSTAC advises the President on policy and technical issues associated with telecommunications and technology. I serve as a member of NSTAC's Industry Executive Subcommittee, and Bob Herbold, our recently retired Executive Vice President and Chief Operating Officer, is a member of President's Information Technology Advisory Committee (PITAC). Thus, Congress can be assured that

Microsoft's commitment to security generally and critical infrastructure protection in particular is supported at the highest levels of the Corporation.

B. Microsoft's Trustworthy Computing Initiative Aims To Increase The Reliability, Security, Privacy, And Integrity Of Computing.

Perhaps most importantly, our chairman and Chief Software Architect Bill Gates spearheads the Trustworthy Computing initiative. This company-wide initiative has four pillars: reliability, security, privacy, and business integrity.

"Reliability" means that a computer system is dependable, is available when needed, and performs as expected and at appropriate levels.

"Security" means that a system is resilient to attack, and that the confidentiality, integrity and availability of both the system and its data are protected.

"Privacy" means that individuals have the ability to control data about themselves and that those using such data faithfully adhere to fair information principles.

"Business Integrity" is about companies in our industry being responsive to customers, helping them find appropriate solutions for their business issues, addressing problems with products or services, and having transparent processes.

We consider the overwhelmingly positive feedback we have received thus far from our customers, outside analysts, Government officials and the press an essential vote of confidence in the direction we have taken. And it is important to note that Trustworthy Computing is not a one-time, limited initiative. Instead, its principles go to the heart of our culture and reflect Microsoft's commitment at all levels of our company to reinforcing the four pillars.

For today's purposes, I want to focus on the security pillar of Trustworthy Computing, where we are working to create products and services that are "Secure by Design, Secure by Default, and Secure by Deployment," - what I call "SD3."

1. "Secure By Design" Means Prioritizing Security In The Product's Initial Design.

"Secure by Design" centers on creating products that are inherently more secure. To accomplish this, we recently provided advanced training to every Windows developer, as well as developers in other parts of the Company, so they could build more secure code and better understand current threats and vulnerabilities. As part of this process, we stopped Windows development for two months to allow more than 8,500 Microsoft developers to conduct an intensive security analysis of millions of lines of Windows source code. We are conducting more threat modeling and more code reviews, including sharing our source code with third parties under our Shared Source program. We are developing code analysis tools to identify flaws that can be exploited. And we are expanding testing of our software by using independent penetration teams and working closely with third party experts.

Another major element of our protection efforts focuses on integrating security features in our products. For example, in Windows XP we installed a personal firewall

and added software restriction policies to allow administrators to limit what software can run on their systems. Both new features help consumers protect themselves from malicious attacks.

2. "Secure By Default" Means Shipping Products With Security Features Enabled.

"Secure by Default" entails shipping products to customers in a locked-down position with features turned off. This means that customers must consciously decide to enable features, leaving other unused services off to narrow the attack surface of a product. We will soon ship a product called Internet Information Server Version 6 this way, and other software packages will follow.

3. "Secure By Deployment" Means Providing Customers With The Most Updated Security Information.

"Secure by Deployment" focuses on making it easier for consumers and IT professionals to maintain systems through improved "security usability" and patch management. Although we have long worked hard to disseminate patches to users quickly and efficiently, we are further improving the process. For example, any Windows XP user can be automatically notified when critical updates are available, and they can then easily locate and install a patch. In the enterprise environment, patches can be downloaded to a Windows Update Server for regression testing and approved patches can then be widely distributed and installed in a process virtually transparent to end-users.

In addition, we have created a fully staffed, highly effective security response organization called the Microsoft Security Response Center. We believe that it is the industry's best such organization. It investigates thoroughly all reported vulnerabilities, then builds and disseminates any needed security updates. In 2001, for instance, we received and investigated over 10,000 reports from our customers. Where we found vulnerabilities – as we did in 60 cases – we delivered updated software through well-publicized web sites and our free mailing list of 260,000 subscribers. For example, the vulnerability that was eventually exploited by Code Red was reported to us in June 2001. We developed a patch in roughly ten days and publicized the patch six weeks prior to Code Red's appearance. We believe that our initial efforts spared many of our customers from being significantly affected by the worm, and we recognize that updated technology such as the Windows XP Automatic Update feature will help protect even more people from similar future attacks.

C. Microsoft Has Participated In A Collaborative Process Of Devising Baseline Security Configurations For Windows 2000 Professional Workstations.

The announcement on July 17, 2002 of a baseline security configuration for Windows 2000 is another example of our commitment to security and demonstrates the positive results that flow from a voluntary public-private partnership. Security experts

from a broad range of public and private organizations including the National Institute of Standards and Technology, the Defense Information Systems Agency, the National Security Agency, the General Services Administration, the SANS Institute, and the Center for Internet Security jointly published recommended consensus baseline security settings for Windows 2000 Professional workstations. Microsoft reviewed the proposed settings as part of its commitment to working with Government and industry experts to create a more trustworthy computing environment.

The recommendations outlined can be used as part of a comprehensive security strategy for Windows 2000 Professional workstations in managed enterprise environments. We welcome the efforts of these Governmental and non-profit entities who are eager to join us in producing a safer computing environment, and we are committed to engaging with industry leaders and governments around the world to identify security threats to computer networks, share best practices, and prevent dangerous computer attacks.

D. Microsoft Works Closely With Government Agencies, Other Industry Members, And Foreign Governments To Prevent And Investigate Cyberattacks.

Microsoft cooperates with Government agencies, other industry participants, and foreign governments on an operational level to prevent and investigate computer intrusions and other attacks. We have been a strong supporter of the Partnership for Critical Infrastructure Security and have worked closely with the Critical Infrastructure Assurance Office, headed by John Tritak, to develop a strong public/private partnership to defend the United States' critical infrastructure. We also support the National Cyber Security Alliance coordinated by Dick Clarke's White House Office of Cyber Space Security, and through the Alliance we will help fund a consumer education Ad Council campaign on cyber-security practices for the home user.

In addition, we are a founding member of the Information Technology - Information Sharing and Analysis Center (IT-ISAC), which coordinates information-sharing on cyber-vulnerabilities among information technology companies and the Government. We support the IT-ISAC's efforts to coordinate with the other existing ISACs because of the interdependencies among our nation's critical infrastructure sectors and the possibility that damage caused by an attack on one sector will have disruptive and perhaps devastating effects on other sectors.

We also work closely with the National Infrastructure Protection Center (NIPC) of the Federal Bureau of Investigation, which plays a key role in preventing and investigating cybercrime. Of course, we do not disclose data unless pursuant to judicial process or other lawful authority, as we need to carefully balance the need to protect public safety with the need to protect the privacy of our customers. Finally, we cooperate with foreign governments who are investigating specific cases of cybercrime and that request evidence in accordance with U.S. law.

The Government is currently considering the creation of the Department of Homeland Security and the consolidation of certain Government organizations with cybersecurity responsibilities. Microsoft supports the Government's efforts to craft the right organizational structure to meet our nation's homeland security and cyber-security challenges and we would like to see a strong cyber-security component n the new Department. One challenge is to help build effective public/private partnerships across a range of sectors in order to foster information-sharing to prevent cyber-attacks and enhance cooperation concerning investigations of cyber-crime.

Information-sharing is indeed a key aspect to public/private partnerships, and progress is being made, but there remain obstacles to the greater sharing of information concerning cyber-vulnerabilities with the Government. We support legislation to facilitate cyber-security information-sharing by granting an exemption from the Freedom of Information Act (FOIA) for information about cyber-vulnerabilities voluntarily shared with the Government. This legislation will lead many companies to answer the Government's call that they provide it with more cyber-security data. Indeed, the legislation currently before the House of Representatives to establish a Department of Homeland Security contains such a FOIA exemption. I believe that this change will strengthen the public/private partnership that is needed for increasing our nation's level of cyber-security.

III. Microsoft Supports Current Government Cyber-Crime Initiatives.

The Government has made great strides in fostering greater awareness of cyber-security issues and building an effective public/private partnership. We of course support the job Richard Clarke is doing as the President's cyber-security advisor and coordinator. He has worked for years to raise the level of concern about cyber-security both in the nation's boardrooms and within government departments.

We applaud the House of Representatives for passing H.R. 3482, the Cyber Security Enhancement Act of 2002. We are pleased in particular that this bill strengthens law enforcement's ability to deter cyber-crime by permitting the United States Sentencing Commission to grant federal judges more flexibility in imposing sentences for cyber-crime. Today, sentences for violations of the Computer Fraud and Abuse Act are in large part determined by calculating actual economic loss, which is often difficult to determine in the cyber-crime context. Although other factors may be considered under existing law, H.R. 3482 more clearly delineates a broader range of relevant issues that should be considered when imposing sentences. For example, the Commission may consider whether judges should impose a sentence based upon factors such as the offender's purpose and the effect of the crime on national security or law enforcement interests.

There are other steps that Microsoft respectfully suggests the Government take to help protect our critical infrastructures against cyber-terrorism: First, we support heightened penalties for cyber-crime. Today, only the proceeds of cyber-crime – not the means to commit the crime – can be forfeited to the Government. We urge that forfeiture also apply to any personal property, such as computer equipment, used or intended to be

used in the commission of cyber-crime. We believe the deterrent effect of expanded forfeiture for cyber-crime will be significant, particularly in the cases of felons who wage cyber-attacks for malicious rather than remunerative reasons. Moreover, it makes no sense to permit convicted hackers to keep the device that they used to harm others. Second, we strongly support increased funding for law enforcement personnel, training, and equipment to prevent and investigate cyber-attacks. These hard-working officials – many of whom are former colleagues of mine – are often short-staffed, under-funded, and lacking the state-of-the-art technology used by cyber-criminals. Increased funding is needed to modernize and place them on par with those they investigate. Additional funding may also help the Government coordinate with state and local law enforcement in preventing and investigating cyber-attacks.

Third, as I mentioned above, we are in a perpetual and accelerating race against hackers, and both the Government and industry need continuously to improve their cyber-security capabilities. For this reason, Microsoft supports increased funding for cyber-security research and development (R&D). The Government should increase its support for basic research in technology and should maintain its traditional support for transferring the results of federally-funded R&D to the private sector so that Government R&D will ultimately increase the cyber-security of the private sector. And the Government must also lead by example, securing its own systems through the use of reasonable security practices.

Fourth, we also believe that greater cross-jurisdictional cooperation among law enforcement is needed for investigating cyber-attacks. Cyber-attackers can easily transit any border, as demonstrated by the *I LOVE YOU* and *Anna Kournikova* viruses and the *Solar Sunrise* attacks, all of which were international in scope. Enhanced law enforcement cooperation across local, state and international borders is vital for law enforcement to prevent and investigate cyber-attacks. We also support an international law enforcement framework that establishes minimum criminal liability and penalty rules for cyber-crime so that cyber-attackers cannot escape punishment for cyber-attacks against the U.S. by seeking refuge outside of our borders.

Finally, our Government is composed of different organizations to deal with crime, espionage, and war. These organizations have different missions and authorities including the Foreign Intelligence Surveillance Act (FISA) for intelligence agencies and the Electronic Communications Privacy Act (ECPA) for law enforcement. However, in the case of cyber-attacks, the motive and identity of a particular cyber-attacker is difficult to ascertain at the onset of an investigation. As a result, the investigation poses issues such as which Government agency should take the lead in responding to the attack and what legal authorities will guide the investigation. The resolution of these issues requires continuing communication and a culture of sharing information as authorized by law. We need to think-through how to structure the Government's efforts most appropriately to prevent and investigate cyber-attacks so that we can address these issues effectively and in real time.

IV. Conclusion

Microsoft pledges to remain a leader in industry efforts to secure products and services. Americans, their government and the critical infrastructures they depend on every day face significant and growing cyber-security challenges. Working with our Government partners and industry peers, we are committed to preempting, catching and prosecuting cyber-criminals to protect the computing experiences of our customers and the cyber-security of our nation.

Thank you.

Mr. HORN. And Mr. Weiss, we are delighted to have you here. He is an executive consultant at KEMA Consulting. Thank you.

STATEMENT OF JOSEPH M. WEISS, EXECUTIVE CONSULTANT, KEMA CONSULTING

Mr. WEISS. Thank you. Mr. Chairman and committee members, thank you for the opportunity to address you about an area I consider vitally important to the economic and national security of America, the cyber-security of our critical infrastructures.

I am a control system engineer. I have spent the past 2 years as the technical lead for the electric power industry, developing and understanding of what is known, and, more importantly, what is not known, about the cyber-security of control systems. The control systems I will be referring to are supervisory control and data acquisition, commonly known as SCADA, distributed controlled systems, DCS, and programmable logic controllers, PLCs.

I have been working with all of the organizations that have a role to play in this area including the government, end users, equipment suppliers, standards organizations, and all other relevant organizations. There are several points I would like to make.

One, control systems are vulnerable to cyber-security intrusions, and in fact have been impacted by electronic intrusions.

Two, cyber-security of control systems affects all industries, not just the critical infrastructure.

Three, IT security technology does not protect control systems.

And, finally, cyber-security technology needs to be developed for control systems, and we do need immediate government funding to make this happen.

Cyber-security has been viewed as an IT or Internet issue. Awareness of control system vulnerabilities is very low. The basic design premise inherent in every control system is the control system would be a stand-alone system, and all control system users would be trusted users. Consequently, these systems have been designed inadvertently to be vulnerable to cyber-intrusions. As long as the control systems are not networked, they are not vulnerable to cyber-intrusions. However, in order to make these systems more productive, these previously stand-alone systems are being networked, including to the Net, making them vulnerable to cyber-intrusions. They are not legacy systems anymore.

Additionally, the vast majority of power plants and substations do not have technology to detect electronic intrusions. There have been more than 20 documented cases where control systems have been electronically impacted either intentionally or unintentionally. At least two cases have resulted in damage to the industrial system and environment. Those are the two you had mentioned.

There have been several confirmed cases of inadvertent denial of service in control systems, including one in a nuclear facility. These weaknesses could be exploited by an intentional adversary. Existing cyber-monitoring technology has not detected any of these cases, and I have had discussions with Carnegie-Mellon CERT; they have not detected any of these incidents.

There are only a handful of suppliers of these systems, and they supply the primary industrial applications: power, water, oil, gas, chemicals, metal refining, paper, pharmaceuticals, food, beverages,

etc. Not only are the systems common, but so are the control system architectures. Consequently, if one industry is vulnerable, they all could be.

Additionally, because you were talking about ISACs, this means that the information on control system vulnerabilities from the different industries could be of interest to the individual industry ISACs. Now, existing cyber-security technology has been developed for business functions in the Internet. Control systems require a degree of timing and reliability not critical for business systems. Because of this, employing existing IT security technology in a control system can range from lack of protection to actually creating a denial of service condition. This has actually occurred in attempting to employ encryption in these systems.

Myself and others working with me have developed an understanding of what is needed to make control systems more secure from cyber-intrusion, but additionally to also make these systems more reliable. Cyber-security technologies need to be developed for control system applications. They include firewalls, intrusion detection, encryption, event logging, etc. They don't apply to control systems. The types of cyber-security projects at university classes Congress has identified to fund, are not applicable to control systems. Understanding a business system is different than understanding a control system.

Government funding is needed to establish test beds. DOE can help be a lead on this. It also requires extending existing NIST-NSA methodology for procurement of desktop computing systems' common criteria to industrial control systems. But this is a very difficult task. There are a number of entities waiting to participate when funding is made available. These include DOE, NIST, NSA, several electric utilities control systems suppliers, and IT security suppliers. We also need to make sure that the transition team from Homeland Security addresses control system cyber-security.

I hope you now have a better understanding of control system vulnerabilities and what technologies are needed to make them less vulnerable.

Thank you for your time and interest. And I would be happy to answer any questions.

Mr. HORN. Thank you very much, Mr. Weiss.

[The prepared statement of Mr. Weiss follows:]

Testimony of
Joseph M. Weiss
Control System Cyber Security Expert
Before the Committee on Government Reform's
Subcommittee on
Government Efficiency, Financial Management and
Intergovernmental Relations
U.S. House of Representatives
July 24, 2002

Control System Cyber Security—Maintaining the Reliability of the Critical Infrastructure

Joseph M. Weiss, P.E.,
Executive Consultant, KEMA Consulting

Thank you for the opportunity to address this committee on what I consider to be a very important topic—the cyber security of the critical industry infrastructures.

Since September 11th, the focus of security in the United States has been on physical terrorist attacks. Cyber security concerns have been directed toward Internet use and networking technology. Dramatic steps are being taken to ensure security against physical attacks and increased emphasis is being placed on securing the Internet and networking systems for traditional IT business systems. However, the same cannot be said for operational control systems. These are the distributed control systems (DCS), programmable logic controllers (PLC), and supervisory control and data acquisition (SCADA) systems that are utilized as the backbone of the global industrial infrastructure. There are only a limited number of suppliers of these systems and they are sold throughout the world. Applications include electric power, water, oil and gas, chemicals, pharmaceuticals, paper, metals refining, auto manufacturing, and food processing. There is a growing threat that cyber attacks on operational control systems could create a crisis for which no one is prepared.

The Threat

Whether security breaches come from organized terrorist attacks, hackers, or even unintentional break-ins, the potential exists for devastating consequences. Yet cyber security in control systems is inadequately being addressed by regulatory agencies and the industries themselves.

Cyber attacks on control systems can be targeted at specific systems or subsystems and can target multiple locations simultaneously from a remote location. Such attacks can directly challenge equipment design and safety limits, causing system malfunctions and shutdowns. Electronic attacks can even impact restoration efforts by manipulating procedures or dynamically changing equipment conditions.

Various cyber security intrusion studies by the Department of Energy and commercial security consultants have demonstrated the cyber vulnerabilities of these systems to unauthorized access. Moreover, many control systems have been designed with architectures that did not account for the wholesale transition from analog to digital

instrumentation or external interfaces to corporate and other outside entities. Consequently, these systems lack the bandwidth to operate reliably in today's environments. There have been several cases where control systems (SCADA and DCS) have had denial of service events because of their lack of control system robustness. Procedures on how to utilize these systems in an appropriate manner are often lacking. As a result, there have been several cases of denial of service on control systems, including in a nuclear facility, because of inadequate procedures.

Background

Networking technology (Ethernet, LANs, WANs) and the use of the Internet are ubiquitous. This technology (open, standards-based networking) was initially applied to business systems and other communication systems where timing was not critical, and the "store and forward" approach was routine or expected. Because it was also recognized that these systems would be sending confidential information over unsecured networks, electronic security was part of the system or application design early in the development of the technology. Process and plant operational systems such as "real time" plant control and SCADA systems were originally designed as proprietary, stand-alone systems where security was provided by physical isolation and limited access control (that is, log-on identification). Now, deregulation, productivity enhancements, corporate desire for control system information through such tools as Enterprise Resource Planning (ERP), and other changes are mandating enormous increases in information sharing. The electric power and other traditionally "isolated" industries are adopting more open, standards-based networking technology and/or the Internet to provide increased information sharing in their operations. It has been assumed that the information will be secure and all users would be trusted users.

Electronic vulnerabilities in operational systems are created by a variety of factors including:

- Equipment suppliers provide modems for remote access as part of their standard system configuration and utilize default passwords.
- Plant staff are reluctant to change default passwords because of operator performance considerations during emergency events.
- Plant and corporate staff use of remote access tools such as PCAnywhere or XWindows.
- Security patches often are not supplied to the end-users or are not applied for fear of impacting system performance.
- Most new control and diagnostic hardware and software are web-enabled.
- Control system networks utilize Internet-based control and diagnostic applications without IT Security being aware.
- Power marketers use the Internet to access DCS and SCADA systems for real-time information.
- Insecure communication protocols exist between control systems.
- Applications of tools such as ActiveX controls are insecure.

Control Systems are Different than IT Systems

The prevailing belief has been that information security technologies, policies, procedures, and standards developed for traditional IT business systems would apply to all systems using networking technologies. However, it has been demonstrated that the real-time nature of operational control systems creates a different set of conditions that has not been adequately addressed by more traditional IT technology approaches.

Traditional IT business systems are non-deterministic and communicate peer-to-peer. Consequently, tasks are performed in a linear manner. This allows these systems to utilize existing security technology such as block encryption algorithms.

Control systems, on the other hand, are deterministic systems and can communicate in multiple ways such as peer-to-peer, one-to-many, many-to-many, etc. A deterministic system is one where processing tasks occur within specific time intervals and processing tasks receive priorities given by the Real-time Operating System (RTOS). These priorities can change during the process. More importantly, timing within each task is constrained and tasks must be performed and completed before the results are needed—faster than the "real-time" process they are controlling.

Several issues that impact information security technology are inherent in control systems.

Timing:

- Timing is sensitive, not only for the entire process, but within each task.
- Tasks, and processes within each task, must be capable of being interrupted and restarted.
- Time delays are unacceptable.
- Reliability of data, data packets, etc. is crucial.
- Minimal resources are available.
- Timing and task interrupts can preclude the use of conventional encryption block algorithms.

Communications:

- Non peer-to-peer communications can preclude the use of digital certificates (timing and resources are also issues that could preclude use of digital certificates for control system applications).

Data Integrity:

- Data integrity is crucial; confidentiality is secondary.

Applying IT security technology in control systems can actually impact performance. Several control system suppliers tried to implement National Institute of Standards & Technology (NIST)-approved encryption algorithms on their systems in a test environment. The algorithms were not designed for the timing issues in control system applications. Consequently, the encryption algorithms impacted the control system timing functions to the point the control systems could not perform their functions.

Control System Vulnerabilities

Many forms of remote access have created control system vulnerabilities to security breaches. Insecure communication protocols between control systems and insecure applications of tools, such as ActiveX controls, cause further risks. Damage can range from loss of confidential data to altering data resulting in erroneous equipment operation or operator information leading to miss-operation. Since operational systems are unique compared to traditional information systems, threats will most likely be from individuals who already understand control systems.

An oft-stated remark is that "when my neighbor gets hit, I will do something." This raises two important points:

- Many facilities have no firewalls or intrusion detection systems. Consequently, they have no means of detecting an electronic intrusion. If they are "hit," the only indication will be the damage caused by the intrusion (this means that the statistics that have been quoted about intrusions do not apply to control systems).
- Control systems have been hacked and, in several instances, damage has occurred. Unlike traditional IT electronic attacks that can be identified and categorized by different computer security organizations, there currently is no process to identify and collect potential control system electronic intrusions.

Control systems generally utilize two operating systems. One is at the operator station that has the capability for role-based access, encryption, and other information security technologies. The other is at the "distributed processing unit," where the sensor information is collected and calculations made in real-time. These RTOS are usually proprietary systems that have been configured with specific prioritization and communication threads. Information security policies have not been included in the kernel of these systems. Consequently, these RTOS do not have the capability to make the requisite calls to authorize, authenticate, or encrypt/decrypt before data is sent. Additionally, RTOS dedicate most of their resources to performing calculations related to system operational performance. Security is viewed as an overhead function.

Control System Issues with Existing Security Technology

Security for control systems faces several specific technological hurdles before the energy and other industries will be protected.

Operating Systems

Security standards and policies need to be incorporated into real-time operating systems. However, incorporating security into the control systems means addressing the timing and task completion/interrupt requirements inherent in control system operations. Currently, there are no requirements for computing resources necessary to implement security technology. The Open Group's Real-time Security Forum (with U.S. Department of Defense participation) is addressing this issue.

Encryption

Current block encryption technology "scrambles" the information of an IT system, but it does not let the user know if the information is correct. Standard encryption works in blocks, which do not address the operational system's timing and interrupt needs. Also, existing encryption solutions do not authenticate the source of the data, an important component for ensuring data integrity when packets of data go from one system to the next.

Stream Ciphers, an encryption solution that lets the system encrypt the information as it is received instead of in one batch, has been developed but still needs to be refined and demonstrated in process controls applications.

Firewalls

Firewalls ensure that the data is coming from a credible source and accepted address, but do not account for data corruption that could occur prior to leaving the control system environment and entering the network. Control systems are custom designed to work between different systems and control the process based on past or expected process experience. Firewall solutions for operating systems would have to determine if the packet information has been corrupted to ensure data integrity.

Intrusion Detection Systems (IDS)

Current IDS solutions were designed to look for the patterns of a traditional, Internet-based IT security breach. IDS solutions have not been designed to meet the needs of control systems, which would have to differentiate between an attack and a process change or problem. Digital fault recorders, transient recorders, scan logs, and alarm recorders monitor abnormalities within the process but not the information system logs. Extending existing state models may provide a starting point that can be used with advanced processing technology such as agents.

Protocols

Protocols in use now were designed to make system interactions as easy and open as possible, which leaves traditional security measures such as authentication and authorization out of the loop. Operating systems will have to find protocols that encourage security while still allowing open communication. A number of groups are exploring working solutions, including: International Electrotechnical Commission Technical Committee 57, Working Group 15; the DNP Working Group; and NIST's Process Controls Security Requirements Forum.

What Needs to be Done

Awareness

Awareness of cyber security control system vulnerability is very low. Cyber security has been viewed as an IT and Internet concern. The IT community does not understand the technical differences between IT and controls. To date, the IT community has not felt the controls market was sufficiently large to engage it. The controls community understands controls. The IT security community understands IT security. There needs to be a "marriage," and it will probably require government "help." This same thought is extended to the funding being made available on cyber security. It is not addressing control systems. Either funding needs to be redirected or new funding needs to be made available to encompass control systems.

There currently have been no overt "drivers" such as regulation or insurance to grab the industry's attention. The Federal Energy Regulatory Commission (FERC) Notice of Public Rulemaking that includes security will hopefully change that view for the utility industry.

Technology Development

There are a number of issues that are under this umbrella.

- **Control system security technology R&D.** This would entail development of firewalls, intrusion detection, encryption, and other technology specifically for control systems.
- **Establishment of control system cyber security test beds.** This would be for developing and evaluating new technology, understanding the potential consequences of cyber intrusions, and understanding what technology is really needed. This can only be done in "field conditions" as opposed to a traditional laboratory setting. DOE could be the focal point.
- **Establishment of a "CERT" for control systems.** Carnegie-Mellon's CERT is not set up to monitor control system intrusions or events. An industry-wide "CERT for control systems" could gather information from the various industries that all use the same technology, making industry-specific Information Sharing and Analysis Centers (ISACs) more useful. This could help dispel the various myths circulating that are not helping the awareness effort. Again, DOE could play an integral part.
- **Extension of NIST Common Criteria methodology for industrial control systems.** This will enable vendors and end-users to confidently verify that their systems meet security requirements. NIST would be an important participant since this builds on existing NIST methodology.
- **Procedure development to secure appropriate interface control.** Refinement of generic procedures and development of additional procedures to cover appropriate remote access and interfaces must be completed systematically.
- **Control System Cyber Security Standards.** Standards need to be developed to address security in an information-sharing environment. NIST would play an important role in this effort.

I am concerned that without taking these actions, our critical infrastructures will be vulnerable to intentional, or even unintentional, events in ways we have not contemplated. Thank you for your time and attention. I would be happy to answer questions.

Joe Weiss

###

Mr. HORN. We now will have the questioning of this Panel One, and later Panel Two. Mrs. Schakowsky has numerous commitments here, and so she can use as much as she wants for questioning.

Ms. SCHAKOWSKY. Thank you. I'm sorry that I've been erratically here, and I also have to leave in a moment. But I wanted to thank you all for your testimony.

I wanted to ask Mr. Weiss one question before I left. I represent a district in Illinois which is the most nuclear State in the country; we rely on nuclear power plants more than any. Your testimony said that even nuclear power plants have had a history of some problem with cyber-security.

And I am curious, I know that nearly 50 percent of all the plants that were tested for mock terrorist attacks failed those tests; that they are vulnerable. My understanding is that did not even include testing for cyber-security and cyber-terrorism that could occur.

First of all, do you know if that is true? And I am wondering if you could elaborate a little bit on the vulnerability of nuclear power plants, and what that might mean in terms of a terrorist intrusion into such a plant.

Mr. WEISS. OK. Let me try and answer a number of those questions. First of all, the issue with the nuclear facility I mentioned was actually in a university reactor. It was one that also has the same type of technology as used in commercial nuclear plants, and it was a procedural issue. Nuclear plants originally were designed to be stand-alone systems. They weren't to be connected anywhere else. The non-nuclear safety systems are starting to be connected to the corporate networks because corporate wants to get information. That is starting to make them vulnerable whereas before they were not vulnerable.

Ms. SCHAKOWSKY. That's non-nuclear.

Mr. WEISS. Pardon?

Ms. SCHAKOWSKY. You said non-nuclear?

Mr. WEISS. In other words, on the non-safety side of the nuclear power plant.

Ms. SCHAKOWSKY. I got you.

Mr. WEISS. The safety side of a nuclear power plant is really not vulnerable, because they are not electronically tied to anything. So you are talking about the non-safety portion of the nuclear power plant. To the best of my knowledge, there has been no cyber-testing of any nuclear plant in the United States to date. That is correct.

Ms. SCHAKOWSKY. Thank you.

Mr. HORN. Thank you very much.

Let us start with Dr. Thomas of the University of Southern California. Do you believe there are any cyber-terrorist threat scenarios that are realistic? If so, how do you believe an attack would occur under those circumstances?

Mr. THOMAS. I think there are two important aspects to that. I think the complexities of a cyber-terrorist attack really warrant our attention in that we are not talking about a 16-year-old kid simply hacking into a secure system. In order to make a cyber-attack happen, a lot of other things have to happen, too. Other security measures have to fail. Those hackers or terrorists need not only to understand how to penetrate a computer system, but they also have

to understand how to work a power plant, how to work air traffic control. They need to have a fairly sophisticated understanding of those kind of aspects in order to make an attack successful.

The second thing I would add to that is that our vulnerabilities are not simply technological. And, in fact, my experience has been, in talking to hackers, that in most cases the way a hacker will invade a system is not by getting online and not by typing in passwords, but is generally by calling up somebody in that organization and conning them out of enough information to get access. It is not uncommon for them to call up a secretary and say, I can't get onto the network, my password isn't working; what is your password? And they give it to them, believing that they are a member of the organization.

There's also reports, in terms of air traffic control, of attacks I think in the U.K., which were not cyber-attacks but rather people who got radios and were able to broadcast signals to planes.

So I think the question of vulnerability, what hackers teach us is we should not just look for the most technologically sophisticated way in, but for the easiest way. And I believe that our vulnerabilities are really, in terms of the design of the system, and what is easy to attack in that system is the place where we really need to shore up and make sure that we have access barriers and so on.

So I foresee, if an attack is going to come, that it is not going to come through some sophisticated programming technique or cyber-attack necessarily, but through a much less technologically sophisticated kind of means.

Mr. HORN. What kind of additional expertise do you believe a hacker would need to control a power grid or a financial transaction?

Mr. THOMAS. I think in order to do that, they are going to have to have some understanding—going to have to have some understanding of how that power plant works, how the financial systems work. We tend to forget when we are talking about cyber-attacks that there are people involved on the other end. And when they see things happening that look suspicious or wrong, they tend to look at those things and understand that, if something is askew, that it needs to be examined more carefully.

There is an example, I think, with SCADA of hackers that were in a system for something like 17 days, and one of the lessons that they learned from that is that once hackers got into this control system for power, they had no idea what to do once they were in there. They had the access, but they had no kind of knowledge or sophistication about how that system worked in order to do anything with it.

So, I think that becomes another critical question of a level of expertise that includes the system they are invading as well as the way to get in.

Mr. HORN. Why do you believe that it is unlikely that a hacker could obtain this additional expertise?

Mr. THOMAS. From what I know of the culture itself, hackers are much more interested in access than they are in what they find once they get into a system. I suppose that there are exceptions.

But for them, the challenge mainly lies in getting in and then moving onto another system and another system and another system.

If they do want something from inside a system, it is usually—when we are talking about the culture itself, they want evidence they have been there. They want something for bragging rights. They want a document. One of the things I write about is the fact that while hackers may be pretty smart about technology, they tend to make terrible criminals. They make a lot of mistakes; they are easily caught. When they do things, particularly involving money, they are oftentimes tracked down very quickly and prosecuted very severely for the crimes that they commit. So I think they tend to not have a kind of criminal frame of mind, even though what they are doing are crimes.

Mr. HORN. In your testimony, you indicate that human intervention is required to control important operations of the Nation's critical infrastructure. Could you provide some specific examples of this?

Mr. THOMAS. One of the examples that I think is worth thinking about that's often cited is air traffic control. And in point of fact, air traffic control information that's passed over a network doesn't control anything. It provides information to controllers who then speak to pilots. Pilots have onboard radar. There are a lot of things that have to go wrong in addition to being hacked in order for a plane to crash.

Another example that was cited in the literature was the idea that terrorists could hack into a cereal manufacturing plant like Kellogg's and dump enormous amounts of iron, for example, in children's cereal and poison our children. The number of things that would have to go wrong in that scenario are myriad. For example, the plant would have to notice—or, not notice that they are running out of iron at an incredible rate. There would have to be no one doing any kind of quality testing to see that the cereal, in fact, tastes like iron. It would have to get out on the shelves and not be recalled.

So those kind of human factors, that kind of testing and that kind of observation doesn't necessarily make that kind of attack impossible, it just makes it highly unlikely that it would succeed or have the kind of impact that people would want it to have if they were engaging in terrorism.

Mr. HORN. Mr. Belcher, you point out the dangers of linking all the components of a company's network together under a single protocol. Do you believe that it is practical to unlink infrastructure control systems from the rest of the company's business systems?

Mr. BELCHER. It probably would not be practical, given other business considerations. They're linking for synergies and deficiencies; they are not linking for security. So, in most cases, probably impractical.

Mr. HORN. In your testimony, you indicate that critical infrastructure companies are experiencing attacks that may be specifically targeting them. Can you describe the type of attacks that they are experiencing?

Mr. BELCHER. The attacks that we monitored over the 6 months alone, for instance, we quantified about 180,000 attacks against the client base and analyzed the characteristics of those attacks. There

are numerous attacks that appear targeted, and we're able to quantify some statistics. Approximately 40 percent of all attacks appear to be going after an individual organization rather than searching the Internet for vulnerabilities. It gives a little bit of insight into the motivation. The attacks run the gamut of intent. Some are inconsequential. Some are done by, obvious, children or other miscreants. Some appear to be going after internal networks, for instance, to go after financial information, credit card numbers, commit fraud, commit theft of property. So they run the gamut.

Mr. HORN. In your testimony, you indicate that critical infrastructure companies are experiencing attacks that may be specifically targeting them. Can you describe any type of these, besides what you had mentioned, quantification?

Mr. BELCHER. Sure. Absolutely. If you look at the profiles of attacks coming across the Internet to individual organizations—for instance, if you look at the activity coming from certain countries within the Middle East, they do by and large favor power and energy as an industry. You can read into the motivations all you want. All we are simply providing is quantifiable numbers in association with those activities.

Mr. HORN. You state that information on the inner workings of the system control and data acquisition is available from public sources. Can you describe those sources and what, in your opinion, can or should be used to limit the availabilty of this data?

Mr. BELCHER. This is relating to some of the questions to Dr. Thomas. We have done assessments, as I mentioned, in both written and verbal of many power and energy companies, probably in the magnitude of 40, assessing their corporate infrastructures and their control systems. And while I agree with the majority of the testimony by the entire panel, anecdotally speaking, showing and demonstrating the viability of connecting to these critical networks, sometimes we get resistance along the same lines of Dr. Thomas saying that even giving access it would be difficult to manipulate the systems, and we completely agree.

In the past we have demonstrated the ability to collect open source information on the systems, including their design all the way to a protocol level to do analysis. We demonstrated the ability to watch the operators in those environments. And more importantly, when asking the people that manage those environments, if I give you access to a foreign utility could you manipulate it, and almost every time they say absolutely. Could you manipulate it to cause damage? Absolutely.

So why would we consider threats against our critical infrastructure not at that level of expertise? If you could hire a professional service team of information security experts to go after an organization and they can demonstrate viable access to the most critical components, why would that not be our threshold to consider for attacks coming from other organizing sponsors?

When you are talking about cyber terrorism, you're talking an absolute sliver of the general volume of attacks that an organization is likely to receive, a very, very small percentage. You have to consider that their expertise would be somewhere in the same range of our expertise.

Mr. HORN. Mr. Alan Paller of SANS Institute, you have identified some of the pressures on commercial software developers that impede their ability to produce secure software, including their manufacturing and distribution processes and their desire to make user friendly products. What actions can developers take to eliminate these pressures and remain competitive?

Mr. PALLER. Scott Charney of Microsoft, laid out a plan that ought to be a model for every one of the software companies and the only reason we don't all stand up and cheer and say we are done is that it is all prospective. You have to buy Microsoft's new systems to get this stuff. So we have maybe 150 million people who we still have to help. So the question is what can they do for the rest of us? And I think the key answer came out in an FTC hearing. A person from Sun described it and it is actually the right answer, and I think Microsoft is doing this with the Defense Department. The key is to have all software delivered for agencies that matter, delivered from a local server where the server is kept up to date with the latest patches. And whenever anyone in that organization needs it—that is the way you do externally, too—whenever anyone needs the software, they get it off that local server. And if they'd set that up so all the rest of the infrastructure could use that, we could move quickly. But again, that is prospective. We still have 150 million boxes we have to fix.

Mr. HORN. What are the risks associated with having a common security configuration benchmark for all Federal systems?

Mr. PALLER. Let me tell you the benefit first and then the risk. There were some tests last week—and before that—that took a regularly installed system and then ran one of the good vulnerabilities testers on it. And they found a certain number of high priority, medium priority and low priority vulnerabilities. Then it installed the minimum benchmark and ran the same tests over again and several tests were run. The average was 80 to 88 percent of all those vulnerabilities disappeared. So that's why you want to do a minimum benchmark.

Then the question is what breaks? The answer is that you don't want to do is break things. The absolute key is you can't install this and cause a critical application to break. And so the difficulty is making sure that something doesn't break. And the next step in these benchmarks is to set up test beds so all application vendors can run their application against the test bed and make sure their customers' applications won't break.

But the answer to your question is the cost is breaking applications. We can't let that happen.

Mr. HORN. You state that so much emphasis has been placed on a risk based approach that many organizations fail to make any investments in security until a risk assessment is completed.

Mr. PALLER. It is true. It is sad. GAO and congressional language is so emphatic that you have to do this risk assessment that people just get at big meetings and say "We can't do anything until we have done a risk assessment and they take a long time and they're buying computers every day. So it is not that they're not buying the computers and installing them. You've just got this huge consulting contract going on and on and on and you are not hardening the boxes you're installing today.

Mr. HORN. What type of security investments do you believe should be made prior to completing a risk assessment?

Mr. PALLER. I think it is very much like living in a really rough neighborhood. You ought to lock the doors at night and maybe all the time when you're in your house and have locks on the windows. And there is a certain small set of things that every computer should have before we allow it—we as users, allow it to be connected to the Internet. If you think of this as unsafe cars on the road, that car could hurt all of us, there ought to be some little thing you do, and the vendors will help. They are coming around and willing to help. But before anyone hooks a machine to the Internet, they need to just lock the doors and lock the windows.

Mr. HORN. Well, you give us some very interesting physical matters rather than just electronic. Mr. Scott Charney of Microsoft might have some ideas on this. Do you have a cascading effect that an attack on one sector of the infrastructure can affect other sectors? And what are some of the challenges in identifying cascading effects across industries?

Mr. CHARNEY. We actually did have such a case when I was at the Justice Department involving a juvenile who had the telecommunications switch in the Town of Worcester, Massachusetts. The switch actually serviced the regional airport where the tower was unmanned. As planes were coming in they would radio the tower and a signal would be sent automatically across the telecommunications network to turn on the landing lights on the runway. As the next plane came in and radioed the tower, because the telecommunications switch was disabled, the landing lights did not go on, the plane was diverted and the airport was closed. So we had a transportation failure based upon an attack on a telecommunications network.

The huge challenge is I don't think anyone would say we fully understand all the interdependencies between all these networks at a granular level. Yes, we all understand if the power supply dies a lot of things won't work. If we don't have telecommunications a lot of things don't work. But how these things actually work in a more granular level where they share vulnerabilities is not entirely clear yet, and there are a lot of groups like the Partnership for Critical Infrastructure Security that are studying that to figure that out.

Mr. HORN. With regard to cascading, please describe the unique problems in recovering from an attack that has cascaded into other sectors.

Mr. CHARNEY. The difficulty, I think, will be in the scope of the problem and integrating all the pieces back together and making sure that all the relevant pieces are in fact considered as we recover from the event. The thought that comes to mind was when I was at PricewaterhouseCoopers, you know, after the September 11th attacks, there was a lot of concern about when the stock markets would be up and operating again. And a lot of people were talking to the exchanges, for example, and the telecommunications carriers. It turns out no one was talking to the exchanges in the back that actually did the actual trading, the clearinghouses for the exchanges, and since then they have become more involved. But people were focused on the obvious visible problem and not some

of the substructures that actually make it all go. So it is really important to understand how the different parts of the infrastructure functions, including the parts that are less visible, and make sure they are all integrated into the recovery plan.

Mr. HORN. What challenges has the Information Technology Information Sharing and Analysis Center encountered in its efforts to coordinate interdependency analysis and recovery efforts with other sectors?

Mr. CHARNEY. I think we have a couple of challenges. One is, of course, that sectors have certain commonalities and therefore we have divided the ISACs into different sectors, but it is important that we not stovepipe the information because of these interdependencies. As a result, in fact there is a meeting later this week, a cross-ISAC meeting where we are starting to coordinate better in that regard. And there are the issues I referred to in my example, the FOIA exemption, and creating an environment where the ISACs can share information far more freely with the government.

Mr. HORN. You mentioned there are these separate organizations and processes to prosecute cyber crimes depending on whether they appear to be intelligence related or law enforcement related. Can you give us a description of some of the differences and how they can affect the outcome of a case?

Mr. CHARNEY. Yes. And some of this goes back to my years at the Justice Department. As you know, historically the government has had different organizations with different authorities to counter different threats. So if you believe you are under attack from a criminal, you launch criminal investigative authorities using things like pen registers, trap and tracers, and wiretaps. When you believe that say an intelligence gathering operation, for example, you have foreign counterintelligence authorities and other tools such as FISA, the Foreign Surveillance Intelligence Act, which, for example, when I was at Justice requires links to an agent of a foreign power, some sort of governmental action. And then of course when you have war, you have U.N. Charter 51 and you have rules for how you engage in warfare.

The difficulty is that all of those mechanisms and procedures depend upon who is attacking you and why. And in an Internet attack, what you normally do not know at the outset is who is attacking you and why. So there is an issue about what kind of response would be appropriate. And let me give you a real life example.

Many years ago when we were gearing up for air strikes against Iraq, we found we had a massive penetration coming from the Middle East into the U.S. Department of Defense, and there was concern this might have been a preemptive strike against our information systems to disrupt our military activities in the area. Fortunately, the military people involved and the Justice involved knew enough to know that where the attack looks like it is coming from may not be where the attack is coming from. But if you see that kind of attack, the question is, is it a foreign state and does it constitute an act of information warfare? And if it does, does that mean you can drop bombs in response? Is that a proportional response under the rules of war?

Of course we didn't do that. We did investigate the case as a criminal matter, and it came back to two juveniles in Cloverdale, California who were looping through the Middle East and hacking the Department of Defense with help from an Israeli.

So we have this problem in that we set up these processes and procedures, but we are in a completely new threat model. And I simply think the government has to really start thinking about this and figuring out what constitutes the right response in an environment where you don't have the facts you need to make the traditional decisions.

Mr. HORN. What lessons learned did Microsoft take away from the company's intensive scrutiny and security analysis of millions of lines of code?

Mr. CHARNEY. That we need to do a lot better and we are going to do a lot better. You know, I have people who say to me now Microsoft is issuing a lot of bulletins about vulnerabilities and an awful large number of patches. Well, if we looked at our code reviews and threat modeling, I would hope that we are issuing a lot of bulletins and patches because we are making the systems more secure and what we have learned is we have to do this right. And the good thing is that markets are now demanding it. National security and public safety concerns are now demanding it. There is a confluence of events that really rewards, I think, companies that recognize that this has to be an industry initiative and a government industry initiative.

Mr. HORN. Thank you very much for enlightening us on that. Our last questions will be for Mr. Joe Weiss. And what can the Federal Government do to improve the security of the SCADA systems and why don't you explain what S-C-A-D-A is?

Mr. WEISS. SCADA—I think it has been used too much now as a euphemism. What I believe we need to worry about are what's called control systems. These are the real-time systems that control processes, whether they are for a power plant, an assembly line, etc. For whatever reason, the term SCADA came out early. It stands for supervisory control and data acquisition. It's simply a type of control system. It is used in certain types of industries. It is usually used where you are trying to gather data from very dispersed facilities. You are not really trying to do significant calculations.

If you are in a refinery, a power plant or a steel mill where you are more concentrated and you are doing much higher levels of calculation, you have things called distributed control systems. If you are in a discrete type of a facility like an assembly line or a parts manufacturer, you are actually using programmable logic controllers. SCADA has been used as a term to lump them together.

Mr. HORN. A lot of it is with inventory movement in the Japanese——

Mr. WEISS. No. If you will, that is really a manufacturing execution system. What we are worried about is the physical control aspect that occurs in real-time. You want to open or close a breaker in a substation. You want to move a valve. You can even think of your sprinkler system at home. The purpose of a control system is to be able to do that in an automated way. It is going to take, for

example, a pressure or a temperature and to make a change in order to keep my process moving the right way.

What has happened is with the net, it has allowed us to get information from so many different places and to use these new, mathematical algorithms to make this adjustment of different signals better and smarter and quicker. And in a sense that's what's opened us up because we can.

Now to the question you asked originally. We have a problem with the chicken and the egg. The chicken and the egg are vendors, and not just in electric utilities, but generally the control system suppliers aren't producing secure control systems because they feel there's no market. It would take development—like I say, the technology isn't even there yet because they are different. It would take development and it would take a lot of other things. So the vendors are not supplying that secure control system.

On the other hand, the end users, be they utilities, oil companies, etc., because the vendors don't have one they don't even put it in their specs. So what's happening is we are in this chicken and egg scenario that we are not moving at all, and that is one area of the government can help us is in a sense getting this market to occur or the fact that there needs to be a market so the technology will even occur.

The other piece is literally the technology development itself. There's an awful lot of technology that's being developed in DOD that may have some relevance to us. The converse is if you look at a ship, the ship is a power plant with a rudder. So there's an awful lot, if you will, of synergy in between. But if the government helps, for example, and is involved with the test beds, the way it will move this forward is to actually have facilities where you can go in and try out and test out and find out what happens when I do put this in, what is my incremental security benefit, what is my either incremental improvement of reliability or possibly decrease in reliability. So I have some intelligent way of saying, what should I do? We don't have that right now.

Mr. HORN. What sectors are most vulnerable and why?

Mr. WEISS. All, because we all have the same control systems from the same vendors using the same architectures. The vulnerability—I am not talking threat. Again, I am a control system engineer talking about the systems. From a vulnerability perspective, the same control system from the same vendor is in power plants, is in refineries, is in water treatment plants, is in steel mills. So in a funny sense, the vulnerability is no different. The threat may be different, but the vulnerability isn't.

Mr. HORN. Let me ask this one last question to this panel. How available are hacking tools? Mr. Weiss, let's just go down the line.

Mr. WEISS. They are available. What we didn't realize is their applicability to a control system. We had originally assumed that it wouldn't impact a control system. We are starting to find out that they can. But let me just add one other thing. In order to impact a control system, you don't need a hacking tool. That, to me, is something that's different. There are other things that you can use to impact, via cyber, the operation of a control system and it doesn't have to be a hacking tool.

Mr. CHARNEY. The tools are widely available. And what that means, of course, is that when you're under attack and under an attack that appears to be sophisticated, it may not be a sophisticated attacker. It may be a novice.

Mr. PALLER. Just to reinforce that, I was the expert witness in the Mafia Boy trial where he attacked Yahoo and eBay and he used a tool that he got from somebody else. He had no clue how the tool worked. And as I said earlier, there are at least 2,000 programs running at all times searching on the whole Internet. And finally there are Web sites now where you can do either of two or three things. You can actually type in what you want a virus to do and it will write the virus for you. You can type in who you want to attack and it will run the attack. Anybody can use those Web sites.

Mr. BELCHER. I think everyone in the panel is going to say I think the tools are readily available. I think the concern would be that for cyber terrorism issues you are really worried about the perpetrator that does not need or does not want the tool.

Mr. THOMAS. I would agree that tools are widely available. And I may have a different perspective in that I would suggest that the availability of tools is not necessarily a bad thing. I think it does force software companies to be responsible in updating their product, in analyzing their own networks and analyzing their own software. And as a result we get better security because those tools are out there, not worse.

Mr. HORN. Well, I want to thank each of you. You have educated all of us in many ways, and so thank you very much and we will now bring panel two forward. If you would like to stay, fine.

Robert Dacey is the Director U.S. General Accounting Office; Ronald Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation; John S. Tritak, Director, Critical Infrastructure Assurance Office, Department of Commerce; Stanley Jarocki, Chairman, Financial Services Information and Analysis Center, and Vice President, Morgan Stanley IT Security. The last part of this is Louis G. Leffler, Manager-Projects, North American Electric Reliability Council. And as you know, gentlemen, a lot of you have been here before. If you have any aides with you just get them to take the oath, also. And Mr. Marc Maiffret, we are glad to have him here.

[Witnesses sworn.]

Mr. HORN. Mark Maiffret will join this panel and there is a sign already for him and a chair and we are glad you made it here. Chief hacking officer and co-founder of eEye Digital Security. And then we will start with you if we might.

STATEMENT OF MARC MAIFFRET, CHIEF HACKING OFFICER AND CO-FOUNDER, eEYE DIGITAL SECURITY

Mr. MAIFFRET. Thank you. Thank you for having me. My name is Marc Maiffret, Chief Hacking Officer and Co-Founder of eEye Digital Security. We focus on creating computer security products, and we are also heavily involved in vulnerability research.

Much debate has been given to the security of our infrastructure. Some are peddling doom and gloom. That sounds like a script to the next cheesy sci-fi movie. Others, however, are ignoring the

problem to say it is overhyped. I personally believe that it is pointless to debate whether our infrastructure is secure or not. At the heart of it all we have the basic understanding that as a Nation we wish to be secure. If our infrastructure is vulnerable, then we are not secure. Therefore, more time needs to be put into creating guidelines of how to secure infrastructure rather than debating whether it is secure or not. With proper guidelines in place and enforced by our government, we will be that much closer to securing our infrastructure.

The current level of security within our infrastructure cannot be judged as a whole. There are too many systems run by too many organizations, therefore making it very hard to quantify how secure or insecure our infrastructure is. The fact does remain, though, that there are vulnerable systems within our infrastructure. It is also a fact that many of the software solutions controlling our infrastructure are vulnerable. This includes the various software that controls SCADA systems.

SCADA systems are probably one of the most vulnerable parts of our infrastructure because of the link created between software and hardware allowing engineers in infrastructure companies to easily manage their systems. A lot of times it is possible to gain access to the networks which House SCADA systems. Once on these networks, it is entirely possible to take control of an infrastructure site and start performing functions just as an operator of the site would.

I will not go into a ton of detail in possible ways of taking over SCADA systems as I have done so in my written testimony. In the end though, it is entirely possible to take control of SCADA systems. Taking control of a SCADA system is not something that any two-bit Internet hacker is going to be able to do. Hacking SCADA systems should not be equated to teenage hackers breaking into Web sites and then mysteriously being able to control a power grid. That is not to say that technology is not moving to make that type of scenario totally unrealistic. However, hacking a SCADA system does take more skill than an average teenage hacker will have.

Security of our Nation's infrastructure is a complex problem because of the integrated nature of our systems even beyond their technical aspects. It is security meets business, meets usability and meets politics, everyone's opinion of how things should be. Albert Einstein once wrote that if we have the courage to decide ourselves for peace we will have peace. I believe the same goes for security. Only when we as a society decide we truly wish to be secure and then follow through in that decision shall we begin to start to attain security.

Once again, I suggest that in order for us to start to secure our infrastructure, we must create guidelines that critical infrastructure companies must follow. These guidelines must be enforced by our government. We must move quickly on securing our infrastructure for I fear if we do not act soon then we will be forced to thrust our infrastructure through nihilistic rebirth, as the only means of becoming secure would be to start over.

Thank you.

[The prepared statement of Mr. Maiffret follows:]

The State of the Nation's Infrastructure Systems
Wednesday, July 24, 2002
Marc Maiffret, CHO, eEye Digital Security

Everyday I wake up to find myself living in a world where the scientist is growing weaker and the pessimist is growing stronger. We are all too caught up in the moment of quick solutions, through finger pointing at weakness within each other, and the fragile systems that are slowly being placed as crucial foundations for our way of life.

With our lives becoming dependent on technology, there comes the need for increased security. Security is something that few technologists and scientists have been trained to think of when developing new ideas that make our lives easier and more convenient. With the lack of security forethought, we are building our future on systems that are insecure, and that will stay insecure until we are able to drastically change how technology is built, until security takes top priority.

The security of our nation's infrastructure is a complex problem that is affected by the inherent fallibility of the software it is built upon, and by the integrated nature of the systems. It is a problem that goes beyond technology to involve human weakness and trust. It is security meets business, meets usability, meets politics, meets everyone's opinion of how things should be. Albert Einstein once wrote: "If we have the courage to decide ourselves for peace, we will have peace". I believe the same goes for security. Only when we, as a society, decide we truly wish to be secure, and follow through with that decision, shall we begin to start to attain security.

Our Infrastructure is Insecure

Advancements in technology are making it easier for businesses to cut costs and increase productivity. These benefits make it very appealing for companies to quickly update their legacy systems to be using the latest and greatest technology available to them. In many cases, however, the underlying technology is flawed, incorrectly managed, or incomplete.

The newer technology being deployed is mostly made up of COTS (Commercial Off the Shelf) software. This software is attractive because it is easy to use and to maintain, but like all other software it contains flaws that can put it at risk for exploitation. The fact that COTS software is so widely available allows it to easily fall into the hands of users with malicious intent. These users have the potential to uncover security flaws, which then put the software and systems built on the software at risk for attack.

While newer technology is often more easily hacked into, we should not discount that older, legacy systems are just as vulnerable. Many times the only thing that keeps legacy systems secure is what is known as "security through obscurity". Since legacy systems are mostly proprietary, people believe criminal users will not have enough knowledge to manipulate and take control of these systems. The idea of security through obscurity, however, has long been proven to be ineffective.

One of the most common technologies in use within our infrastructure is SCADA (Supervisory Control and Data Acquisition). SCADA is the term that describes the majority of systems which have control over the physical aspects of our infrastructure. In its simplest form, SCADA allows software to manage various hardware aspects of our infrastructure, such as the ability to use software to control part of a power grid or a water treatment plant. Combined with other software that allows for remote control of SCADA software, companies have the capacity to manage their infrastructure with never-before-seen ease. For instance, fifteen field offices can be managed from one central location.

The remote management capability of SCADA systems is where some of the vulnerability of our infrastructure first arises. Most often, the remote management of SCADA systems is implemented using COTS software. Some COTS software applications provide dial-up solutions for remote access to SCADA systems. Others allow employees of infrastructure companies to remotely access and manage SCADA systems via encrypted "tunnels" through the Internet.

Most of these remote management systems attempt to put at least some access control on who is able to use them. This access control is usually implemented in the form of login passwords, and sometimes secure ID tokens. Unfortunately, no matter how strong the system to restrict access, we must remember that COTS software providing the access has been found time and time again to contain flaws. A weakness in the connecting software can be manipulated to bypass standard access control and provide direct access to the SCADA software itself.

Beyond the COTS software that provides "add-on" functionality to the SCADA software in the form of remote management, sometimes common software applications make up the backbone of SCADA systems. Technologies such as Microsoft Windows or Oracle databases have been proven insecure in the past, and thus compromise the security of the entire infrastructure system as a whole.

COTS software is not the only thing that can lead to attackers being able to gain access to SCADA systems; many times the software actually driving SCADA systems is flawed. I have been able to analyze a few SCADA software packages in a lab environment and have found that most of them actually contain possible vulnerabilities that can lead to SCADA systems being compromised.

With the use of backend database systems and network redundancy via common protocols, there exists a potentially attackable communication mechanism between some SCADA software. This communication mechanism is often flawed and vulnerable to common types of security vulnerabilities such as buffer overflow attacks and database injection attacks. In addition, SCADA software sometimes insecurely stores password information, which is a crucial component for any sort of final access control that may be in place. So, not only does an attacker have the ability to gain access to a SCADA network via COTS vulnerabilities, he then can elevate his access within SCADA control software via weak password storage mechanisms.

--

The vulnerability of our infrastructure to external attack does not only apply to networks where remote access to SCADA is in place. In fact, the infrastructure sites that do not employ any remote access capabilities are equally at risk. This usually exists because of improper segmentation of networks - infrastructure sites do not have the right systems in place to separate their corporate networks from their critical infrastructure networks.

Many times two networks will exist at a single infrastructure site. One network is put in place to facilitate the control of the site via SCADA, and one network for supporting employees at the site not directly working with the SCADA systems. A security risk can arise when these two networks are not properly segmented. For instance, even though the SCADA system may not be directly connected to the Internet, an attacker coming through the Internet can compromise a computer within the non-SCADA side of the network and then jump to the SCADA part of the network. From their remote location, the attacker would be able to take advantage of the functionality that SCADA offers to seize control of a power plant, a water treatment plant, a dam, or even an amusement park.

--

A final, important weakness of SCADA software is the lack of auditing capabilities. Auditing functionality allows companies to keep an eye on what is happening within their computing environment. A consistent audit of the system

provides a way for companies to trace the events that occur after a breach in security, which in turn provides crucial information required for quickly assessing and repairing any damage to the system. Also, auditing offers organizations a way to keep an eye on employees which could potentially be working for outside entities that wish to cause harm.

Beyond the obvious security needs at the software and network level, one cannot ignore the need for personal and physical security at infrastructure facilities. Even with the best computer security in place there will always be employees who must have access to the systems. While processes like auditing help keep tabs on employees potentially abusing infrastructure systems, more needs to be done on a social level to ensure the security of our infrastructure.

Know Your Enemy

At the human level, security must begin from the inside out. Not only should infrastructure companies keep watch for malicious employees, but all employees should be given proper training regarding proper security practices.

In order to start to attain security within the internal workings of a company you must establish a level of trust. This trust needs to be proven and enforced. We have become a society where nothing and no one is as it seems, and the strict enforcement of honesty and integrity on the operators of our nation's infrastructure is a necessity.

The threat of an attack from a person inside an organization must be considered, but not always are these internal attacks intentional. An outside attacker may often times target a social weakness within an infrastructure employee. By playing off of that weakness, it is possible that foreign persons can manipulate an employee to perform actions which ultimately lead to harm being brought against the network or the infrastructure. This type of social attack is something that has been used by the intelligence community for a long time, as it usually can lead to quicker and more significant turnaround on the effort expended for such tasks.

Although social attacks can be a useful method for getting into critical systems, not every enemy of ours posses the skills needed to perform such an attack. For those that cannot compromise our infrastructure via social or physical means, they could most likely do so via technology exploits as discussed earlier. The ability to penetrate our infrastructure through vulnerabilities in technology is a real threat that must be taken seriously, especially since it is likely to be the easiest and most appealing method of attack for many.

Attacking our infrastructure via technical means can be appealing because it can be done anonymously and without much money. The anonymous aspect stems from the way our communication systems have been built with the idea of access from anywhere, at anytime. It can be cumbersome to try and find the origin of an attack coming through a network, because of the ability to cover one's tracks without much effort. Also, with

advancements in wireless technology and its widespread adoption, the ability to be invisible is easier than ever.

The second thing that makes hacking into infrastructure appealing is that computer hacking is the Wal-Mart of espionage and terrorism. It is a rather cheap endeavor, and the supply of trainable hackers is nearly endless. So far, however, I would guess that terrorists are only recently starting to realize the benefits of having people within their organizations that have real hacking skills.

It should be made clear that not every hacker is able to break into an infrastructure company and shut down a power grid. I have seen one too many news articles written that portray your average teenage computer hacker as having the ability to reach the most sensitive of systems - this is simply not true. It would be rare for the average hacker or script kiddie (so named because they rely upon existing pieces of hacking code – or scripts – that circulate around the Internet) to have the technical and social skills needed to break into something like a power grid. We shouldn't assume that script kiddies will never get access to SCADA networks – they have in the past – it is just very unlikely. Because of the complexity involved, only a small number of people in this country actually have the skills needed to perform such a targeted attack.

On the other hand, countries like China and Russia have been working hard to keep their hacking abilities on par with the United States. A country with the hacking ability of China should be considered a formidable foe and not be taken lightly. At the moment it could very well be that the only thing keeping our infrastructure safe from such countries is the simple fact that those countries have not wished to attack us. A race between the United States and other countries to increase their technical hacking capabilities could be reminiscent of the nuclear arms race between the United States and Russia. Although, not nearly as potentially devastating.

Starting From Zero

I think one of the things working to our advantage is the fact that we are essentially starting from nothing. The technology we are building upon is truly in its infancy, and the existing security is spotty at best. There is a lot that we can start to do to secure our infrastructure, which personally I believe is a good position to be in. We've yet to exhaust all possibilities of things we can do to protect ourselves from attack.

We must start small and build up. One of the first things we should be doing to protect our infrastructure is to enforce a set of requirements on the security of sites and companies that we deem to be integral parts of our critical infrastructure. A lot of industries are slowly starting to move in the direction of forcing businesses to meet a certain level of security. The healthcare industry has begun to force hospital networks to come up to a standardized level of security. We should be doing the same with our infrastructure companies.

Infrastructure companies must be held accountable and forced to meet a set of security standards. We must also understand that infrastructure companies in many areas are struggling, and the increased costs of security must be taken into consideration. The financial aspect of such an endeavor, while an obviously important topic, must not overtake the importance of security. Once again, we must all agree to be secure, and follow through. Also, we should not simply let people write off their lack of security due to expenses - security at the most basic level does not need to be expensive.

To outline the requirements of what it takes to secure an infrastructure site is a bit beyond the scope of this paper. There definitely should be a meeting held to formalize an enforceable best-practice security policy for infrastructure companies. This should not simply be a meeting of management, but of employees as well, and of various knowledgeable people from the security community. Far too often we overlook the amazing insight of the people who "work in the trenches". I have talked with many employees at infrastructure companies who know all too well what is wrong with their systems, and often know what needs to be done to fix it.

Listed below are a few high-level ideas that should be covered when setting security requirements for infrastructure companies:

- Background checks on all employees within critical infrastructure companies. In some cases background checks to the level of checking done to get some government clearances.
- Specifications to define a level of security for networked aspects of infrastructure companies.
- Specifications to define a level of security for SCADA control software.
- Specifications to define a level of physical security at infrastructure facilities.

Once again these ideas simply touch on the areas a security requirements policy would cover. These guidelines, once fully created, should be enforced by our government and companies need to be held accountable if they do not meet the requirements.

In the End

The doom and gloom that infrastructure critics have been peddling is not accurate for our current situation. Although weaknesses do exist that can currently be exploited, I believe we are in a fine position to create a thorough and strong security plan to come out on top. Time definitely is of the essence, however, and we should start proactively securing our infrastructure before it is too late.

I do not like hearing that there is no such thing as a secure system. We must believe that we can be secure. Maynard James Keenan once wrote: "The only way to fix it is to flush it all away. Time to bring it down again. Don't just call me pessimist. Try and read between the lines". I fear that if we do not begin to enforce security as a whole, and if we piece together security solutions only as they are needed, then we will be

forced to thrust our infrastructure technology through a nihilistic rebirth, as the only means of becoming secure would be by starting over.

Marc Maiffret
Chief Hacking Officer
eEye® Digital Security

One Columbia
Aliso Viejo, CA 92656
949-349-9062

Mr. HORN. Thank you. That is very helpful and we go now with Robert Dacey, the Director of Information Security, U.S. General Accounting Office, which is under the Comptroller General of the United States. And we always use GAO in one way or the other, beginning or end. You are on the beginning but we will probably ask you what did we miss at the end. And so, Bob, nice to have you here.

STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Mr. DACEY. Mr. Chairman, I am pleased to be here today and thank you for your continuing interests and efforts to provide oversight over this critical area. Today I would like to discuss the challenges that our Nation faces concerning critical infrastructure protection, or CIP, and Federal information security. As you requested, I will briefly summarize my written statement.

We have made numerous recommendations over the last several years concerning CIP and Federal information security challenges that need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in the process, including a number of efforts by other members of this panel. However, much more is needed to address them. These challenges include, No. 1, developing a national CIP strategy. A more complete strategy is needed that will address specific roles, responsibilities and relationships for all CIP entities, clearly define interim objectives and milestones and set timeframes to achieve them and establish appropriate performance measures.

Last week, we issued a report that further highlights the importance of coordinating the dozens of Federal entities involved in cyber CIP efforts. The President's National Strategy for Homeland Security, also released last week, calls for interim cyber and physical infrastructure protection plans by September of this year to be followed at an unspecified date by a comprehensive national infrastructure plan.

The second major challenge is improving analysis and warning capabilities. More robust analysis and warning capabilities are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats. The National Strategy for Homeland Security calls for major initiatives to improve our Nation's analysis and warning capabilities that include enhancing existing capabilities within the FBI and building new capabilities at the proposed Department of Homeland Security.

The third major challenge is improving information sharing on threats and vulnerabilities. Information sharing needs to be enhanced both within the Federal Government and between the Federal Government and the private sector and State and local governments. The National Strategy for Homeland Security identifies partnering with non-Federal entities as a major initiative and discusses the need to integrate information sharing within the Federal Government and among the various levels of government and the private industry. Information sharing and analysis centers, which will be discussed today, continue to be a key component of that strategy. The strategy also discusses the need to use available public policy tools such as grants and regulations.

The fourth challenge is addressing pervasive weaknesses in Federal information security. Despite the importance of maintaining the integrity of confidentiality and availability of important Federal computer operations, Federal computer systems have significant pervasive information security weaknesses. A comprehensive strategy for improving Federal information security is needed in which roles and responsibilities are clearly delineated, appropriate guidance is given, regular monitoring is undertaken and security information and expertise are shared. As I testified earlier this year before this subcommittee, continued authorization of government information security reform legislation is essential to sustaining agency efforts to identify and correct these significant weaknesses.

The President's draft legislation on the creation of a Department of Homeland Security and the National Strategy for Homeland Security acknowledge the need to address many of these challenges. However, much work remains to effectively respond to them. Until a comprehensive and coordinated strategy is developed for all CIP efforts, our Nation risks not having an appropriate and consistent structure to deal with the growing threats of attacks on its critical infrastructures.

Mr. Chairman, this concludes my oral statement, and I would be pleased to answer any questions that you or members of the subcommittee might have.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10:00 a.m. EDT
Wednesday,
July 24, 2002

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges Need to Be Addressed

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-02-961T

United States General Accounting Office July 24, 2002

CRITICAL INFRASTRUCTURE PROTECTION
Significant Challenges Need to Be Addressed

Highlights of GAO-02-961T, testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, House Committee on Government Reform.

Why GAO Did This Study

The explosion in computer interconnectivity, while providing great benefits, also poses enormous risks. Terrorists or hostile foreign states could launch computer-based attacks on critical systems to severely damage or disrupt national defense or other critical operations.

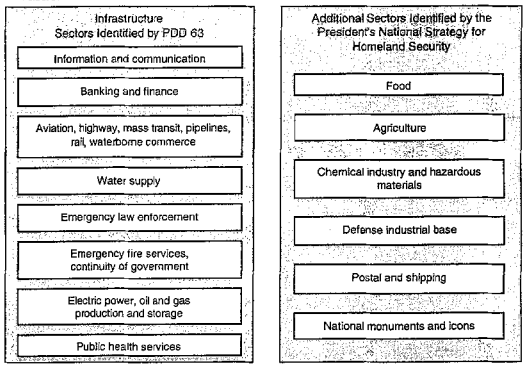
Presidential Decision Directive 63 and Executive Order 13231, issued in 1998 and 2001, respectively, call for various actions to improve our nation's critical infrastructure protection (CIP), including establishing partnerships between the government and the private sector. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety.

The President's national strategy for homeland security, issued last week, identifies protecting critical infrastructures and intelligence and warning, a critical CIP component, as two of six mission areas and expands our nation's approach to cover additional sectors of our economy (see graphic). At the subcommittee's request, GAO discussed challenges the nation faces in protecting our critical infrastructures and addressing federal information security.

What GAO Found

Prior GAO work has identified and made recommendations concerning several CIP challenges that need to be addressed:

- *Developing a national critical infrastructure protection strategy.* A more complete strategy is needed to define specific roles, responsibilities, and relationships for all CIP organizations and to establish objectives, timeframes, and performance measures. The President's national strategy calls for more detailed CIP plans.
- *Improving analytical and warning capabilities.* More robust analytical and warning capabilities are still needed to identify threats and provide timely warnings, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information.
- *Improving information sharing.* Information sharing needs to be enhanced both within the government and between the federal government and the private sector.
- *Addressing pervasive weaknesses in federal information security.* A comprehensive strategy for improving federal information security is needed, in which roles and responsibilities are clearly delineated, appropriate guidance is given, regular monitoring is undertaken, and security information and expertise are shared to maximize their value.



This is a test for developing highlights for a GAO report. The full testimony, including GAO's objectives, scope, methodology, and analysis, is available at *www.gao.gov/cgi-bin/getrpt?GAO-02-961T.* For additional information about this testimony, contact Robert F. Dacey (202-512-3317). To provide comments on this test highlights, contact Keith Fultz (202-512-3200) or E-mail *HighlightsTest@gao.gov.*

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the challenges that our nation faces concerning critical infrastructure protection (CIP) and federal information security. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety. Federal agencies and other public and private entities rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information. Further, protecting against computer-based attacks on critical infrastructures is an important aspect of homeland security. Earlier this month, we testified on the proposed transfer of certain government agencies associated with protecting our nation's critical infrastructures to the Department of Homeland Security.[1] Congress has held numerous hearings on this subject, passed legislation, and issued reports[2] that have been instrumental in ensuring appropriate oversight and focus.

Today, as requested, I will provide an overview of the federal government's approach to protecting our nation's critical infrastructures that is described in Presidential Decision Directive (PDD) 63, Executive Order 13231, and the newly issued national strategy for homeland security.[3] I will also provide an overview of cyber threats and vulnerabilities. Next, I will discuss the challenges, identified in prior GAO work, that the nation continues to face in implementing CIP and consequently in protecting our homeland, as well as protecting federal information systems. These challenges are (1) developing a more complete national CIP strategy, (2) improving analysis and warning capabilities, (3) building on information sharing efforts, and (4) addressing the pervasive nature of federal information security weaknesses.

In preparing this testimony, we relied on prior GAO reports and testimonies on critical infrastructure protection, information security, and national preparedness, among others. We also met with officials at the Department of Commerce's Critical Infrastructure Assurance Office and the Federal Bureau of Investigation's (FBI) National Infrastructure

[1] U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Homeland Security Challenges Need To Be Addressed* GAO-02-918T (Washington, D.C.: July 9, 2002).

[2] *Security in the Information Age, New Challenges, New Strategies*, Joint Economic Committee, United States Congress, May 2002.

[3] *National Strategy for Homeland Security*, Office of Homeland Security, July 2002.

Protection Center to follow up on prior recommendations and to discuss their proposed move to the new department. We also reviewed the national strategy for homeland security released last week. Our work was performed in accordance with generally accepted government auditing standards.

Results in Brief

We have identified and made numerous recommendations over the last several years concerning several critical infrastructure protection and federal information security challenges that need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, much more is needed to address them. These challenges include:

- *Developing a national CIP strategy.* A more complete strategy is needed that will address specific roles, responsibilities, and relationships for all CIP entities; clearly define interim objectives and milestones; set time frames for achieving objectives; establish performance measures; and include all relevant sectors. Last week, we issued a report that further highlights the importance of coordinating the many entities involved in cyber CIP efforts.[4] The President's national strategy for homeland security, also issued last week, calls for interim cyber and physical infrastructure protection plans by September 2002 and a comprehensive national infrastructure plan to be completed by the Department of Homeland Security. The strategy does not indicate when this comprehensive plan will be completed. Until a comprehensive and coordinated strategy is developed for all CIP efforts, our nation risks not having a consistent and appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.
- *Improving analysis and warning capabilities.* More robust analysis and warning capabilities, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats. The national strategy for homeland security calls for major initiatives to improve our nation's analysis and warning capabilities that include enhancing existing capabilities at the FBI and building new capabilities at the proposed Department of Homeland Security.
- *Improving information sharing on threats and vulnerabilities.* Information sharing needs to be enhanced both within the government and between the federal government and the private sector and state and local

[4] U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

governments. The national strategy for homeland security identifies partnering with nonfederal entities as a major initiative and discusses the need to integrate information sharing within the federal government and among federal, state, and local governments and private industry. The strategy also discusses the need to use available public policy tools, such as grants.

- *Addressing pervasive weaknesses in federal information security.* Because of our government's and our nation's reliance on interconnected computer systems to support critical operations and infrastructures, poor information security could have potentially devastating implications for our country. Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems have significant pervasive information security weaknesses. A comprehensive strategy for improving federal information security is needed, in which roles and responsibilities are clearly delineated, appropriate guidance is given, regular monitoring is undertaken, and security information and expertise are shared to maximize their value.

Although the national strategy for homeland security acknowledges the need to address many of the challenges discussed above, much work remains to successfully implement it. The President's draft legislation on the creation of a Department of Homeland Security would create an information analysis and infrastructure protection division to address many of these challenges. Earlier this month, we testified on the potential benefits and challenges of the proposed transfer. In addition, the Comptroller General has recently testified on key issues related to the successful implementation of, and transition to, the new Department of Homeland Security.[5]

Critical Infrastructure Protection Policy Has Been Evolving Since the Mid-1990's

Federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990's. Over the years, a variety of working groups have been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. In October 1997, the President's Commission on Critical Infrastructure Protection issued its report,[6] which described the potentially devastating implications of poor information security from a national perspective. The report recommended several measures to achieve a higher level of critical infrastructure protection, including

[5] *U.S.* General Accounting Office, *Homeland Security: Critical Design and Implementation Issues,* GAO-02-957T (Washington D.C.: July 17, 2002).

[6] *Critical Foundations: Protecting America's Infrastructures,* Report of the President's Commission on Critical Infrastructure Protection (Oct. 1997).

infrastructure protection through industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyberthreats." It said that the FBI had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In 1998, the President issued PDD 63, which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated lead agencies to work with private-sector and government organizations. Further, it established CIP as a national goal and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, no later than 2003, an enhanced capability.

To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;
- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and

- the National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.[7]

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. The infrastructures are (1) information and communications; (2) banking and finance; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. The special functions are (1) law enforcement and internal security, (2) intelligence, (3) foreign affairs, (4) national defense, and (5) research and development. For each of the infrastuctures and functions, the directive designated lead federal agencies, known as sector liaisons, to work with their counterparts in the private sector, known as sector coordinators. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electrical power industry. Similarly, regarding special function areas, the Department of Defense (DOD) is responsible for national defense, and the Department of State is responsible for foreign affairs.

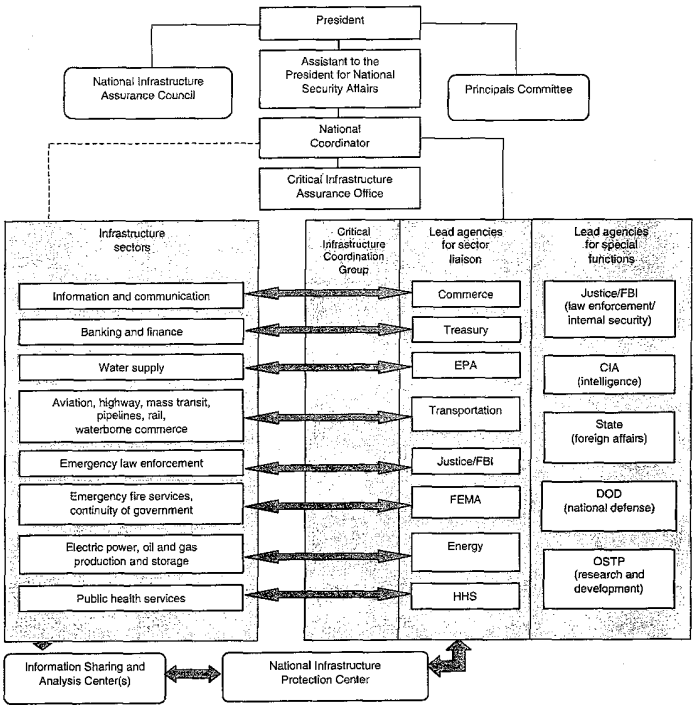
PDD 63 called for a range of actitivites intended to establish a partnership between the public and private sector to ensure the security of infrastructures essential to the operations of the government and the economy. It required that the sector liaison and the sector coordinator work with each other to address problems related to CIP for their sector. In particular, PDD 63 required them to (1) develop and implement a vulnerability awareness and education program and (2) 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 major attacks; and
- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstitute minimum essential capabilities in the aftermath of an attack.

[7]Executive Order 13231 replaces this council with the National Infrastructure Advisory Council.

To facilitate private-sector participation, PDD 63 also encouraged the voluntary creation of information sharing and analysis centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Figure 1 displays a high-level overview of the organizations with CIP responsibilities as outlined by PDD 63.

Figure 1: Organizations with CIP Responsibilities as Outlined by *PDD 63*



Note: In February 2001, the Critical Infrastructure Coordination Group was replaced by the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee on Counter-terrorism and National Preparedness. In October 2001, the National Infrastructure Assurance Council was replaced by the National Infrastructure Advisory Council, and cyber CIP functions performed by the national coordinator were assigned to the chair of the President's Critical Infrastructure Protection Board.

Source: CIAO.

In January 2000 the White House issued its *National Plan for Information Systems Protection*.[8] The national plan provided a vision and framework for the federal government to prevent, detect, respond to, and protect the nation's critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements. Subsequent versions of the plan were expected to (1) define the roles of industry and state and local governments working in partnership with the federal government to protect physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

In October 2001, President Bush signed Executive Order 13231, establishing the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures. The Special Advisor to the President for Cyberspace Security chairs the board. Executive Order 13231 tasks the board with recommending policies and coordinating programs for protecting CIP-related information systems. The executive order also established 10 standing committees to support the board's work on a wide range of critical information infrastructure efforts. The board is intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications that were assigned to the Office of Homeland Security by Executive Order 13228, dated October 8, 2001. According to Executive Order 13231, the board recommends policies and coordinates programs for protecting information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems. The Special Advisor reports to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security. In addition, the chair coordinates with the Assistant to the President for Economic Policy on issues relating to private-sector systems and economic effects and with the Director of the Office of Management and Budget (OMB) on issues relating to budgets and the security of federal computer systems. In addition, Executive Order 13231 reiterated the importance and voluntary nature of the ISACs but did not suggest additional activities for the ISACs.

Last week, the President issued the national strategy for homeland security to "mobilize and organize our nation to secure the United States homeland from terrorist attacks." According to the strategy, the primary objectives of homeland security in order of priority are to (1) prevent terrorist attacks within the United States, (2) reduce America's

[8]The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* (Washington, D.C.: 2000).

vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur. The strategy identifies critical infrastructure and intelligence and warning, a critical component of CIP, as two of six mission areas; the strategy states that if terrorists attack one or more pieces of our critical infrastructure, they may disrupt entire systems and cause significant damage to the nation. The other four mission areas are border and transportation security, domestic terrorism, defending against catastrophic terrorism, and emergency preparedness and response.

Implementing PDD 63 Has Not Been Completely Successful

Both GAO and the inspectors general have issued reports highlighting concerns about PDD 63 implementation. As we reported in September 2001, efforts to perform substantive, comprehensive analyses of infrastructure sector vulnerabilities and the development of related remedial plans had been limited. Further, a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in federal agencies' implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by December 2000, and (2) develop procedures and conduct vulnerability assessments.[9] Specifically,

- many agency CIP plans were incomplete, and some agencies had not developed such plans;
- most agencies had not completely identified their mission-essential infrastructure assets; and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective inspectors general reviews.[10] Further, OMB reported in February 2002 that it planned to direct all large agencies to undertake a Project Matrix review to identify critical infrastructure assets and their interdependencies with other agencies and the private sector.[11]

[9]The PCIE primarily is composed of the presidentially appointed inspectors general and the ECIE is primarily composed of the agency head-appointed inspectors general. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 inspectors general of their respective agencies' PDD 63 planning and assessment activities.

[10]GAO-01-822, September 20, 2001.

[11]Project Matrix is a CIAO methodology that identifies all critical assets, nodes, networks, and associated infrastructure dependencies and interdependencies.

We identified several other factors that had impeded the efforts of federal agencies to comply with PDD 63. First, no clear definitions had been developed to guide development and implementation of agency plans and measure performance. For example, PDD 63 established December 2000 as the deadline for achieving an initial operating capability and May 2003 for achieving full operational capability of key functions. However, the specific capabilities to be achieved at each milestone had not been defined. The PCIE/ECIE report noted that agencies had used various interpretations of initial operating capability and stated that, without a definition, there is no consistent measure of progress toward achieving full security preparedness. In addition, several agency officials said that funding and staffing constraints contributed to their delays in implementing PDD 63 requirements. Further, the availability of adequate technical expertise to provide information security has been a continuing concern to agencies.

Cyber Threats Are Increasing and Infrastructure Sectors Are Vulnerable

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, and national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

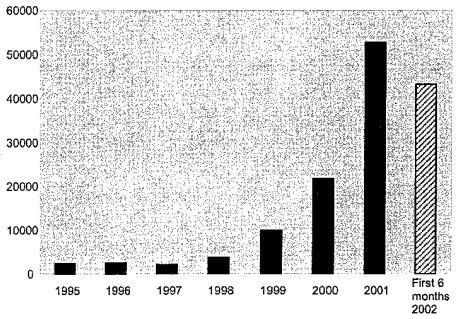
Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly

becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. In addition, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions.

Reports of attacks and disruptions abound. The 2002 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 43,136 for just the first six months of 2002.[12] And these are only the reported attacks. The CERT® Coordination Center estimates that as much as 80 percent of actual security incidents go unreported, in most cases because the organization was unable to recognize that its systems had been penetrated or because there were no indications of penetration or attack. Figure 2 shows the number of incidents reported to the CERT® Coordination Center from 1995 through the first six months of 2002.

[12]CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Figure 2: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center: 1995-the first six months of 2002



Source: Carnegie-Mellon's CERT® Coordination Center

Since the September 11 attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, earlier this year, the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups such as al Qaeda have used the Internet to launch a known attack on the United States infrastructure, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan. Further, in his October congressional testimony, Governor James Gilmore, former Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (commonly known as the "Gilmore Commission"), warned that systems and services critical to the American economy and the health of our citizens—such as banking and finance, "just-in-time" delivery systems for goods, hospitals, and state and local emergency services—could all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.[13] The national strategy for homeland security states that terrorist groups are already

[13]Testimony of Governor James S. Gilmore III, former Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction before the House Science Committee, October 17, 2001.

exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely.

Each of the sectors' critical infrastructures is vulnerable in varying degrees to natural disasters, component failures, human negligence, and willful misconduct. Several examples are highlighted below.

- In 1997, the *Report of the President's Commission on Critical Infrastructure Protection* stated that treated water supplies did not have adequate physical protection to mitigate the threat of chemical or biological contamination, nor was there technology available to allow for detecting, identifying, measuring, and treating highly toxic, waterborne contaminants. It added that cyber vulnerabilities include the increasing reliance on Supervisory Control and Data Acquisition (SCADA)[14] systems used to monitor and control equipment for control of the flow and pressure of water supplies. Several weeks ago, the President of the Association of Metropolitan Water Agencies testified that water utilities are increasingly reliant on information systems to control many aspects of water treatment and distribution and stressed the importance of conducting research into methodologies and technologies to detect, prevent, and respond to acts of terrorism against drinking water systems. In addition, on January 30, 2002, NIPC issued an information bulletin on terrorist interest in water supply and SCADA systems. It stated that a computer that belonged to an individual with indirect links to bin Laden contained structural architecture computer programs that suggested that the individual was interested in structural engineering as it related to dams and other water-retaining structures. The bulletin further stated that U.S. law enforcement and intelligence agencies have received indications that al Qaeda members have sought information on SCADA systems that is available on multiple SCADA-related web sites.
- The President's 1997 Commission also reported on the physical vulnerabilities for electric power related to substations, generation facilities, and transmission lines. It further added that the widespread and increasing use of SCADA systems for control of energy systems provides increasing capability to cause serious damage and disruption by cyber means. Riptech, a Virginia-based security firm, recently released an Internet security threat report for the period of January 1, 2002, to June 30, 2002, that was based on information from a sample of its client

[14]SCADA systems allow utility operators to monitor and control processes that are distributed among various remote sites. This connectivity offers increased accessibility and ease of operations for legitimate users, but also could expose the utility to cyber intruders.

organizations.[15] Riptech concluded that companies in the energy industry, along with financial services and high-tech companies, experience the highest rate of overall attack activity. According to the study, power and energy firms received an average of 1,280 attacks per company and 70 percent of them had at least one severe attack during the period studied. Riptech has also reported on the vulnerabilities of SCADA systems.

- In February 2002, the National Security Telecommunications Advisory Committee and the National Communications System released a document, *An Assessment of the Risk to the Security of the Public Network*, relating to the vulnerabilities of the telecommunications sector. This report concludes that (1) the overall vulnerability of the public network to electronic intrusion has increased, (2) government and industry organizations have worked diligently to improve protection measures, (3) the threat to the public network continues to grow as it becomes a more valuable target and the intruder community develops more sophisticated capabilities to launch attacks against it, and (4) continuing trends in law enforcement and legislation have increased the ability of the government and the private sector to deter the threat of intrusion. The report says that the implementation of packet-based next-generation network technologies, including wireless, and their convergence with traditional networks have introduced even more vulnerabilities into the public network.

Not only is cyber protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has recently been highlighted as a major concern. In fact, NIPC has stated that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For example, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack.

Understanding the many interdependencies between sectors is also critical to the success of protecting our national infrastructures. According to a report by the CIP Research and Development Interagency Working

[15] For the 6-month period, Riptech analyzed firewall logs and intrusion detection system alerts. From these initial data, more than 1 million possible attacks were isolated and more than 180,000 confirmed.

Group,[16] the effect of interdependencies is that a disruption in one infrastructure can spread and cause appreciable impact on other infrastructures.[17] The report also stated that understanding interdependencies is important because the proliferation of information technology has made the infrastructures more interconnected, and the advent of competition, "just in time" business, and mergers among infrastructure owners and operators have eroded spare infrastructure capacity. In congressional testimony earlier this month, the director of Sandia National Laboratories' Infrastructure and Information Systems Center stated that these interdependencies make it difficult to identify critical nodes, vulnerabilities, and optimized mitigation strategies.

The Nation Faces Ongoing CIP Challenges

For years, we have reported on and made numerous recommendations to improve the protection of our critical infrastructures and federal information systems. Specific challenges that the nation faces include developing a more complete national CIP strategy, improving analysis and warning capabilities, improving information sharing, and addressing pervasive weaknesses in federal information security.

National CIP Strategy Needs to Be Developed

A clearly defined strategy is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. An underlying issue in the implementation of PDD 63 is that no national strategy yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities and defines interim objectives.[18] We have reported since 1998 on the need for such a strategy. Just last week we issued a report making additional recommendations about what should be included in this strategy.[19] The national strategy for homeland security calls for interim cyber and physical infrastructure protection plans by September 2002 and a comprehensive national infrastructure plan to be completed by the Department of Homeland Security. The strategy does not indicate a date when this comprehensive plan is to be issued.

[16]The CIP Research and Development Interagency Working Group was established in March 1998 to develop and sustain a roadmap on what technologies should be pursued to reduce vulnerabilities of and counter threats to our critical infrastructures.

[17]*Report on the Federal Agenda in Critical Infrastructure Protection Research and Development, Research Vision, Objectives, and Programs*, CIP Research and Development Interagency Working Group, January 2001.

[18]GAO-01-822, September 20, 2001.

[19]GAO-02-474, July 15, 2002.

GAO Has Long Recognized the Need for a National CIP Strategy

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.[20] At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0. An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures by achieving three crosscutting infrastructure protection objectives:

- minimizing the possibility of significant and successful attacks;
- identifying, assessing, containing, and quickly recovering from an attack; and
- creating and building strong foundations, including people, organizations, and laws, for preparing, preventing, detecting and responding to attacks.

However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role. Subsequently, in July 2000, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate; (2) who should be held accountable for their success or failure; and (3) whether such activities will effectively and efficiently support national goals.[21]

A May 2001 White House press statement announced that the administration was reviewing how it was organized to deal with

[20]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).

[21]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation*, GAO/T-AIMD-00-268 (Washington, D.C.: July 26, 2000).

information security issues and that recommendations would be made on how to structure an integrated approach to cyber security and CIP. Specifically, the announcement stated that the White House, federal agencies, and private industry had begun to collaboratively prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and review how the government is organized to deal with information security issues.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives are to be met, as well as guidelines for measuring progress.[22] Accordingly, we made several recommendations to supplement those we had made in the past, including those regarding NIPC. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in CIP and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

National Strategy Needs to Define Relationships among the Key CIP Organizations and Include All Sectors

In a report issued last week, we identified at least 50 organizations involved in national or multiagency cyber CIP efforts.[23] These entities include 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations. These organizations are primarily located within 13 major departments and agencies mentioned in PDD 63.[24] Other departments and agencies, in addition to the 13 mentioned in PDD 63, are also involved in CIP activities. For example, the Department of Interior has cyber and

[22] GAO-01-822, September 20, 2001.

[23] GAO-02-474, July 15, 2002.

[24] These are the Departments of Commerce, Defense, Energy, Justice, Transportation, Health and Human Services, State, and Treasury; and the Environmental Protection Agency, the Federal Emergency Management Agency, the General Service Administration, and the National Science Foundation.

physical safeguard responsibilities associated with dams and the Department of Agriculture has responsibilities for food safety. Also, in addition to the over 50 organizations identified, agencies have cyber CIP activities specific to their department's systems, and other cyber security organizations receive federal funding. In addition, our review did not cover organizations with national physical CIP responsibilities like Transportation's Office of Pipeline Safety; Treasury's Bureau of Alcohol, Tobacco, and Firearms; and the Environmental Protection Agency's Chemical Emergency Preparedness and Prevention Office. Appendix I provides a high-level organization chart of the organizations we reviewed and more a detailed figure on component organizations' involvement, including a description of the type of CIP activities they perform. Appendix II displays in tabular format the entities and their activities.[25]

A clearly defined strategy is also essential for clarifying how CIP entities coordinate their activities with each other. Although most organizations in our review could identify relationships with other key cyber CIP entities, relationships among all organizations performing similar activities (e.g., policy development, analysis and warning) were not consistently established. For example, under PDD 63, the CIAO was set up to integrate the national CIP plan, coordinate a national education and awareness program, and coordinate legislative affairs. Nevertheless, of the organizations conducting policy development activities, only about one-half reported that they coordinated with the CIAO. Executive Order 13231, *Critical Infrastructure Protection in the Information Age,* acknowledged the need for additional coordination among organizations involved in cyber CIP by creating the President's Critical Infrastructure Protection Board to coordinate federal efforts and programs related to the protection of critical infrastructures. It is also important that any CIP-related efforts or proposals outside the scope of PDD 63 be coordinated with other CIP efforts. For example, we understand that EPA is considering a proposal that would require the 15,000 industrial facilities using hazardous chemicals to submit detailed vulnerability assessments.

Further, our report stated that an important aspect of this strategy will be the inclusion of additional potentially relevant critical infrastructure sectors or federal agencies sectors that are not included in PDD 63. As mentioned previously, PDD 63 identifies 8 sector infrastructures with 13 lead agencies associated with the 8 sectors and 5 special functions. However, PDD 63 did not specifically address other possible critical sectors such as food supply, chemical manufacturing, and delivery

[25]Appendix I displays the five general CIP activities according to a color-coded legend. Appendix II provides an alternative (table format) for black and white printing.

services and their respective federal agency counterparts. Executive Order 13231 also did not change the sector infrastructures identified in PDD 63.

However, a few organizations stepped forward to address these gaps. For example, the Department of Agriculture, with responsibilities for food safety, recently established a Homeland Security Council, a departmentwide council with the mission of protecting the food supply and agricultural production. Also, a food ISAC has been recently formed by the Food Marketing Institute in conjunction with NIPC. Further, the chemical ISAC was established earlier this year.

We recommended in our July 2002 report, which was provided to the administration in May for comment, that when developing the strategy to guide federal CIP efforts, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the Special Advisor to the President for Cyberspace Security ensure that, among other things, the strategy

- includes all relevant sectors and defines the key federal agencies' roles and responsibilities associated with each of the sectors, and
- defines the relationships among the key CIP organizations.

The newly issued national strategy for homeland security identifies 14 industry sectors, including the 8 identified in PDD 63. They are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons.

National Strategy for Homeland Security Calls for the Development of Both Interim CIP Plans and a Comprehensive Plan

The national strategy for homeland security calls for interim cyber and physical infrastructure protection plans by September 2002, which are to be completed by the Office of Homeland Security and the President's Critical Infrastructure Protection Board. The strategy also states that the Department of Homeland Security would, building from the September plans, develop a comprehensive national infrastructure plan. The Department of Homeland Security strategy does not indicate a date when the comprehensive plan is to be completed.

According to the strategy, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local government and

the private sector. The plan is to establish standards and benchmarks for infrastructure protection and provide a means to measure performance. The strategy also states that the Department of Homeland Security would unify the currently divided responsibilities for cyber and physical infrastructure. As we have previously recommended, this plan needs to clearly define the roles, responsibilities, and relationships among the many CIP organizations. Until a comprehensive and coordinated strategy is completed that identifies roles and responsibilities for all CIP efforts, our nation risks not having a consistent and appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.

Analysis and Warning Capabilities Need to Be Improved

Another key challenge is to develop more robust analysis and warning capabilities. NIPC was established in PDD 63 as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent. Similar activities are also called for in the President's proposal for the Information Analysis and Infrastructure Protection division.

In April 2001, we reported on NIPC's progress in developing national capabilities for analyzing threat and vulnerability data and issuing warnings, responding to attacks, among others.[25] Overall, we found that while progress in developing these capabilities was mixed, NIPC had initiated a variety of critical infrastructure protection efforts that had laid a foundation for future governmentwide efforts. In addition, NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical capabilities that PDD 63 asserted are needed to protect the nation's critical infrastructures had not yet been achieved, and NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

[25] U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

At the time of our review, NIPC had issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. In addition, it had issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

We reported that the use of strategic analysis to determine the potential broader implications of individual incidents had been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

We reported last year that three factors hindered NIPC's ability to develop strategic analytical capabilities:

- First, there was no generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Second, NIPC had sustained prolonged leadership vacancies and did not have adequate staff expertise, in part because other federal agencies had not provided the originally anticipated number of detailees. For example, at the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of NIPC's 3-year existence. In addition, NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.
- Third, NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work, only three industry assessments had been partially completed, and none had been provided to NIPC. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

To provide a warning capability, NIPC had established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. We reported that NIPC's ability to issue warnings promptly was impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks; (2) a shortage of skilled staff; (3) the need to ensure that NIPC does not raise undue alarm for insignificant incidents; and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

In addition, NIPC's own plans for further developing its analysis and warning capabilities were fragmented and incomplete. The relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council were unclear regarding who had direct authority for setting NIPC priorities and procedures and providing NIPC oversight. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

In our report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and
- clearly define the role of NIPC in relation to other government and private-sector entities.

NIPC's director recently told us, in response to our report recommendations, that NIPC had developed a plan with goals and objectives to improve its analysis and warning capabilities and that NIPC has made considerable progress in this area. For example, the director told us that the analysis and warning section has created two additional teams to bolster its analytical capabilities: (1) the critical infrastructure

assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community. The director added that NIPC (1) now holds a quarterly meeting with senior government leaders of entities that it regularly works with to better coordinate its analysis and warning capabilities; (2) has developed close working relationships with other CIP entities involved in analysis and warning activities, such as the Federal Computer Incident Response Center (FedCIRC), DOD's Joint Task Force for Computer Network Operations, the Carnegie Mellon's CERT® Coordination Center, and the intelligence and anti-virus communities; and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation.

The director also stated that NIPC has received sustained leadership commitment from key entities, such as CIA and the National Security Agency, and that it continues to increase its staff primarily through reservists and contractors. The director acknowledged that our recommendations are not fully implemented and that despite the accomplishments to date, much more work remains to create the robust analysis and warning capabilities needed to adequately address cyberthreats.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been focused on cyber threats. In April 2001, we reported that while PDD 63 covers both physical and computer-based threats, federal efforts to meet the directive's requirements have pertained primarily to computer-based threats, since this was an area that the leaders of the administration's CIP strategy viewed as needing attention. As we have stated earlier, swarming attacks, that employ concurrent cyber and physical attacks, are an emerging threat to the U.S. critical infrastructure.

The director told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC has developed thresholds with several ISACs for reporting physical incidents and has, since January 2002, issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability will be a significant challenge.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and

law enforcement communities. For example, considerable debate has ensued in recent weeks regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, with the President's proposed separation of NIPC from the FBI's law enforcement activities, including the Counterterrorism Division and NIPC field agents, it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the proposed new Department of Homeland Security are effective and that appropriate information is exchanged on a timely basis.

In addition, according to NIPC's director, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI recently testified that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds requires a centralized and robust analytical capacity that does not currently exist in the FBI's Counterterrorism Division. He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations requires an enhanced analytical and data mining capacity that is not presently available. Also, NIPC's director stated that multiagency staffing, similar to NIPC, is a critical success factor in establishing an effective analysis and warning function and that appropriate funding for such staff was important.

The national strategy for homeland security identifies intelligence and warning as one of six critical mission areas and calls for major initiatives to improve our nation's analysis and warning capabilities, including enhancing existing capabilities at the FBI and building new capabilities at the proposed Department of Homeland Security. The strategy also states that currently there is no government entity responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. Such responsibility would be given to the new Department of Homeland Security under the President's proposal. Further, the strategy states that the Department of Homeland Security is to have broad statutory authority to access intelligence information, as well as other information, relevant to the terrorist threat. In addition, the strategy indicates that the department would turn this information into useful warnings.

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The

President's national strategy for homeland security also states that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy states that the U.S. government does not perform vulnerability assessments of all the nation's critical infrastructure. It further states that new Department of Homeland Security would have the responsibility and capability of performing these comprehensive vulnerability assessments.

Government Faces Information Sharing Challenges

Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we testified in July 2000,[27] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

Last October we reported on information sharing practices that could benefit CIP.[28] These practices include

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;,
- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory changes.

In June of this year, we also reported on the information sharing barriers confronting homeland security, both within the federal government and with the private sector.[29]

[27] GAO/T-AIMD-00-268, July 26, 2000.

[28] U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[29] U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing Into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002).

A number of activities have been undertaken to build relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish information sharing and analysis centers (ISACs). For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members included representatives from private industry, other government agencies, state and local law enforcement, and the academic community. Currently, NIPC reports over 5,000 InfraGard members.

PDD 63 encouraged the voluntary creation of ISACs that could serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. ISACs are critical since private-sector entities control over 80 percent of our nation's critical infrastructures. While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities which the ISACs could undertake, including:

- establishing baseline statistics and patterns on the various infrastructures;
- serving as a clearinghouse for information within and among the various sectors;
- providing a library for historical data for use by the private sector and government; and
- reporting private-sector incidents to NIPC.

In April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships and that NIPC had undertaken a range of initiatives to foster information sharing relationships with ISACs, as well as government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us that a new ISAC development and support unit had been created, whose mission is to enhance private-sector cooperation and trust, resulting in a two-way sharing of information. NIPC now reports that over 10 ISACs have been established, including those for the chemical industry, surface transportation, electric power, telecommunications, information

technology, financial services, water supply, oil and gas, emergency fire services, food, and emergency law enforcement. Officials informed us that the center has signed information sharing agreements with most of these ISACs, including those representing telecommunications, information technology, water supply, food, emergency fire services, banking and finance, and chemical sectors. NIPC officials added that most of these agreements contained industry-specific cyber and physical incident reporting thresholds. Further, officials told us that NIPC has developed a program with the electric power ISAC whereby members transmit incident reports directly to the center. Table 1 lists both the PDD 63 sectors and additional sectors that the administration has acknowledged in its national strategy for homeland security, the lead federal agencies associated with each, ISACs that have been established according to NIPC, and ISACs that have entered into information sharing agreements with NIPC.

Table 1: Lead Agencies and ISAC Status by CIP Sector

Sectors identified by PDD 63 in 1998	Lead agency as designated in the national strategy for homeland security	ISAC established	Information sharing agreements with NIPC
Information and Telecommunication	Department of Homeland Security*		
Information technology		✓	✓
Telecommunications		✓	✓
Banking and finance	Department of the Treasury	✓	✓
Water	Environmental Protection Agency	✓	✓
Transportation	Department of Homeland Security*		
Air transportation			
Surface transportation		✓	
Waterborne commerce			
Emergency law enforcement**	Department of Homeland Security*	✓	✓
Emergency fire services,** continuity of government	Department of Homeland Security*		
Emergency fire services		✓	✓
*Continuity of government****			
Energy	Department of Energy		
Electric power		✓	✓
Oil and gas		✓	
Public health	Department of Health and Human Services		
New sectors identified in national strategy for homeland security			
Food	Department of Agriculture, Health and Human Services	✓	✓
Meat and poultry			
All other food products			
Agriculture	Department of Agriculture		
Chemical industry and hazardous materials	Environmental Protection Agency	✓	✓
Defense industrial base	Department of Defense		
Postal and shipping	Department of Homeland Security		
National monuments and icons	Department of the Interior		

*The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigations, and the Federal Emergency Management Agency.

**In the new national strategy for homeland security, emergency law enforcement and emergency fire services are included in an emergency services sector.

***In the new national strategy for homeland security, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.

Despite progress establishing ISACs, more needs to be done. Each sector does not have a fully established ISAC, those that do have varied participation, and the amount of information being shared between the federal government and private sector organizations also varies.

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. Many suggest that the government should model the Year 2000 Information and Readiness Disclosure Act, which provided limited exemptions and protections for the private sector in order to facilitate the sharing of information on Year 2000 readiness.

Other obstacles to information sharing, which were mentioned in recent congressional testimony, include difficulty obtaining security clearances for ISAC personnel and the reluctance to disclose corporate information. In recent congressional testimony, the Director of Information Technology for the North American Electric Reliability Council stated that the owners of critical infrastructures need access to more specific threat information and analysis from the public sector and that this may require either more security clearances or declassifying information.[30] The chief technology officer for BellSouth testified that an additional concern of the private sector in sharing information is the disclosure of sensitive corporate information to competitors.[31] Also, we previously reported that officials representing state and local governments, as well as the private sector, have concerns about funding homeland security.[32]

The private sector has also expressed its concerns about the value of information being provided by the government. For example, the President for the Partnership for Critical Infrastructure Security stated in congressional testimony earlier this month that information sharing between the government and private sector needs work, specifically, in

[30] Testimony of Lynn P. Constantini, Director, Information Technology, North American Electric Reliability Council, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2002.

[31] Statement of Bill Smith, Chief Technology Officer, BellSouth, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2002.

[32] U.S. General Accounting Office, *Homeland Security: Key Elements to Unify Efforts Are Underway, But Uncertainty Remains*, GAO-02-610 (Washington, D.C.: 2002).

the quality and timeliness of cyber security information coming from the government.

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cyber security problems and solutions that are essential to protecting our nation's critical infrastructures. The national strategy for homeland security, which outlines 12 major legislative initiatives, includes "enabling critical infrastructure information sharing." It states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate its voluntary submission. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and state and local governments. Actions have been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.

Public policy tools will surely be discussed and reviewed as we look for additional means of improving information sharing. In the Comptroller General's testimony several weeks ago, he stated that intelligence and information sharing challenges highlight the need for strong partnerships with those outside the federal government and that the new department will need to design and manage tools of public policy (e.g., grants to nonfederal entities) to engage and work constructively with third parties.[33] We have previously testified on the choice and design of public policy tools that are available to governments.[34] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. As we have reported, the design of federal policy will play a vital role in determining the use of and success of such tools in protecting the homeland. Some of these tools are already being used. For example, the Environmental Protection Agency recently announced that approximately 400 grants will be provided to assist large drinking water utilities in assessing their vulnerabilities. Consistent with the original intent of PDD 63, the national strategy for

[33]GAO-02-866T, June 25, 2002.

[34]U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO 02-549T (Washington, D.C.: Mar. 28, 2002).

homeland security states that, in many cases, sufficient incentives exist in the private market to supply protection of America's critical infrastructures. However, the strategy also discusses the need to use available policy tools to raise the security of our critical infrastructures. For example, it mentions federal grants programs to assist state and local efforts, legislation to create incentives for the private sector, and regulation.

Information sharing within the government also remains a challenge. In April of last year, we reported that NIPC and other government entities had not developed fully productive information sharing and cooperative relationships. For example, federal agencies had not routinely reported incident information to NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's FedCIRC. Further, NIPC and DOD officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. According to NIPC's director, the relationship between NIPC and other government entities has significantly improved since our review, and that the quarterly meetings with senior government leaders have been instrumental in improving information sharing. In addition, officials from the Federal Computer Incident Response Center and the U.S. Secret Service in testimony have discussed the collaborative and cooperative relationships that now exist between their agencies and NIPC.

Pervasive Weaknesses in Federal Information Security Need to Be Addressed

At the federal level, cyber CIP activities are a component, perhaps the most critical, of a department or agency's overall information security program. Federal agencies have significant critical infrastructures that need effective information security to adequately protect them. However, since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[35] Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 agencies

[35] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

had significant information security weaknesses.[36] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[37] More current analyses of audit results, as well as of the agencies' own reviews of their information security programs, continue to show significant weaknesses that put critical federal operations and assets at risk.

Weaknesses Remain Pervasive

Our November 2001 analyses of audit results for 24 of the largest federal agencies showed that weaknesses continued to be reported in each of the 24 agencies.[38] These analyses considered GAO and inspector general (IG) reports published from July 2000 through September 2001, which included the first annual independent IG evaluations of agencies' information security programs required by government information security reform legislation (commonly referred to as "GISRA").[39]

Our analyses showed that the weaknesses reported for the 24 agencies covered all six major areas of general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of

[36] U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000).

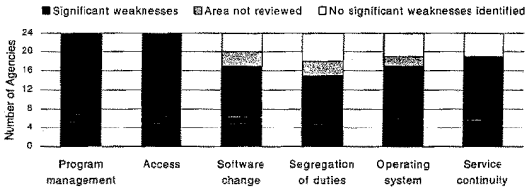
[37] U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update*, GAO/HR-99-1 (Washington, D.C.: Jan. 1999); *High-Risk Series: An Update*, GAO-01-263 (Washington, D.C.: Jan. 2001).

[38] U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001).

[39] Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, October 30, 2000. Congress enacted "GISRA" to supplement information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by OMB and the National Institute of Standards and Technology, as well as audit and best practice guidance issued by GAO. Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establishes new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. Effective November 29, 2000, GISRA is in effect for 2 years after this date.

duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 3 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 3: Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued July 2000 through September 2001.

As in 2000, our current analysis shows that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively. For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In 2001, we also found that 19 of the 24 agencies (79 percent) had weaknesses in service continuity controls (compared to 20 agencies or 83 percent in 2000). These controls are particularly important because they ensure that when unexpected

events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission.

Our current analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 3 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as the departments of Defense and Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. In response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems is also likely to increase as agencies review and evaluate their information security programs as required by GISRA.

Weaknesses Pose Substantial Risks for Federal Operations, Assets, and Confidentiality

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Examples from recent audit reports issued in 2001 illustrate the serious weaknesses found in the agencies that continue to place critical federal operations and assets at risk:

- In August, we reported that significant and pervasive weaknesses placed Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.[40] Commerce's IG has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.[41]

[40] U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*, GAO-01-751 (Washington, D.C.: Aug. 13, 2001).

[41] Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements, Inspector General Audit Report No. FSD-12849-1-0001.

- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than $12 billion annually in payments, that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.[42]

- In March, we reported that although DOD's Departmentwide Information Assurance Program made progress, it had not yet met its goals of integrating information assurance with mission-readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.[43]

- In February, the Department of Health and Human Services' IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[44] Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which, during fiscal year 2000, was responsible for processing more than $200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data (such as Medicare enrollment, eligibility, and paid claims data) and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

To correct reported weaknesses, several agencies took significant steps to redesign and strengthen their information security programs. For example, the Environmental Protection Agency has moved aggressively to reduce the exposure of its systems and data and to correct weaknesses we

[42]U.S. General Accounting Office, *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk*, GAO-01-615 (Washington, D.C.: July 3, 2001).

[43]U.S. General Accounting Office, *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program*, GAO-01-307 (Washington, D.C.: Mar. 30, 2001).

[44]Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000, A-17-00-00014, Feb. 26, 2001.

identified in February 2000.[44] While we have not tested their effectiveness, these actions show that the agency is taking a comprehensive and systematic approach that should help ensure that its efforts are effective.

Agencies' GISRA Results Also Highlight Weaknesses

As required by GISRA, agencies reviewed their information security programs, reported the results of these reviews and the IGs' independent evaluations to OMB, and developed plans to correct identified weaknesses. These reviews and evaluations showed that agencies have not established information security programs consistent with GISRA requirements and that significant weaknesses exist. Although agency actions are now underway to strengthen information security and implement these requirements, significant improvement will require sustained management attention and OMB and congressional oversight.

In its fiscal year 2001 report to the Congress on GISRA, OMB notes that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security.[45] In particular, the report highlights six common security weaknesses: (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

In general, our analyses of the results of agencies' GISRA reviews and evaluations also showed that agencies are making progress in addressing information security, but that none of the agencies had fully implemented the information security requirements of GISRA and all continue to have significant weaknesses. In particular, our review of 24 of the largest federal agencies showed that agencies had not fully implemented requirements to

- conduct risk assessments for all their systems;

[44] U.S. General Accounting Office, *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk*, GAO/AIMD-00-215 (Washington, D.C.: July 6, 2000).

[45] Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform* (Feb. 2002).

- establish information security policies and procedures that are commensurate with risk and that comprehensively address the other reform provisions;
- provide adequate computer security training to their employees including contractor staff;
- test and evaluate controls as part of their management assessments;
- implement documented incident handling procedures agencywide;
- identify and prioritize their critical operations and assets, and determine the priority for restoring these assets should a disruption in critical operations occur; or
- have a process to ensure the security of services provided by a contractor or another agency.

H.R. 3844 would permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA, which is to expire on November 29, 2002. As demonstrated by its first-year implementation, GISRA proved to be a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. Agencies have noted benefits from GISRA, such as increased management attention to and accountability for information security. In addition, the administration has taken important actions to address information security into the President's Management Agenda Scorecard. We believe that continued authorization of such important information security legislation is essential to sustaining agency efforts to identify and correct significant weaknesses. Further, this authorization would reinforce the federal government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

Improvement Efforts are Underway, But Challenges to Federal Information Security Remain

Information security improvement efforts have been undertaken in the past few years both at an agency and governmentwide level. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed. Accordingly, it is important that federal

information security efforts be guided by a comprehensive strategy for improvement.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security. This strategy should also consider other organizations with information security responsibilities, including OMB, which oversees and coordinates federal agency security, and interagency bodies like the CIO Council, which are attempting to coordinate agency initiatives. It should also describe how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[47] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Implementing such standards for federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

Third, ensuring effective implementation of agency information security and CIP plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA, would allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and

[47]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

monitoring process established through these provisions is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective. Moreover, with GISRA expiring on November 29, 2002, we believe that continued authorization of information security legislation is essential to improving federal information security.

The implementation of GISRA has also resulted in important actions by the administration, which if properly implemented, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment. The administration also has plans to

- direct all large agencies to undertake a review to identify and prioritize critical assets within the agencies and their interrelationships with other agencies and the private sector, as well as a cross-government review to ensure that all critical government processes and assets have been identified;
- integrate security into the President's Management Agenda Scorecard;
- develop workable measures of performance;
- develop e-training on mandatory topics, including security; and
- explore methods to disseminate vulnerability patches to agencies more effectively.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for

computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As stated by the director of the CERT® Coordination Center in congressional testimony last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches."[48] In addition, in its December 2001 third annual report, the Gilmore Commission recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.[49]

In conclusion, prior GAO work has identified and made recommendations concerning several CIP challenges that need to be addressed. These include

- completing a comprehensive and coordinated CIP strategy that includes both cyber and physical aspects, defines the roles and responsibilities of the many CIP organizations, and establishes objectives, timeframes, and performance measures;
- improving analysis and warning capabilities to address the potential disruption of both cyber and physical threats and vulnerabilities;
- improving information sharing both within the federal government and between the federal government and the private sector and state and local governments, and
- addressing pervasive weaknesses in federal information security.

Although the President's national strategy for homeland security discusses many of these challenges, much work remains to effectively address them.

[48]Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, U.S. House Committee on Government Reform, September 26, 2001.

[49]*Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Dec. 15, 2001).

The CIP plans that are expected to be released in September and the comprehensive CIP plan to be completed at a later date are important steps in protecting our critical infrastructures. However, even more critical to protecting our country against terrorism is successfully implementing these plans.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at daceyr@gao.gov.

Appendix I

Organizations Involved in National or Multiagency CIP Activities

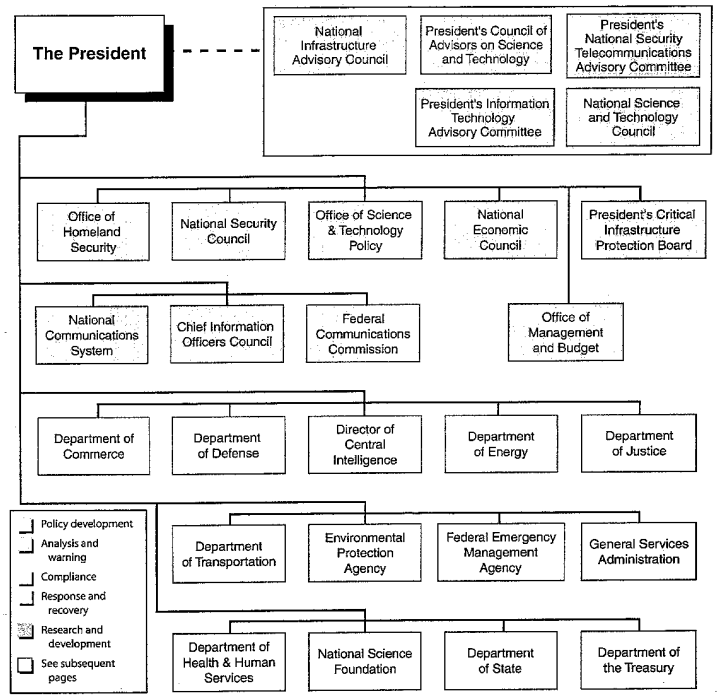
Although each organization involved in our review of national or multiagency cyber critical infrastructure protection (CIP) efforts described a wide range of cyber CIP related activities, collectively they described activities related to the following five categories:[50]

- policy development, including advising on policy issues, coordinating and planning CIP activities, issuing standards and best practices, providing input to the national CIP plan, developing education and outreach programs with governmental and private sector organizations, and coordinating internationally;
- analysis and warning, including conducting vulnerability analyses, gathering intelligence information, coordinating and directing activities to detect computer-based attacks, disseminating information to alert organizations of potential and actual infrastructure attacks, and facilitating the sharing of security related information;
- compliance, including overseeing implementation of cyber CIP programs, ensuring that policy is adhered to and remedial plans are developed, and investigating cyberattacks on critical infrastructures;
- response and recovery, including reconstituting minimum required capabilities, isolating and minimizing damage, and coordinating the necessary actions to restore functionality; and
- research and development, including coordinating federally sponsored research and development in support of infrastructure protection.

Figure 4 displays a high-level overview of the organizational placement of the 5 advisory committees; 6 Executive Office of the President organizations; 13 executive branch departments and agencies; and several other organizations involved in national or multiagency cyber CIP efforts. For departments and agencies, figure 5 provides further detail on component organizations' involvement, but does not illustrate the internal relationships within each agency. For all figures, organizations' cyber CIP-related activities are identified in one or more of the five general categories discussed above.

[50]GAO-02-474, July 15, 2002.

Figure 4: Overview of National or Multiagency Federal Cyber CIP Organizations



Note: Major agencies or departments are highlighted in yellow here and on the following pages. The organizations are color-coded to correspond to one or more of the five general activities related to cyber CIP (see legend on figures).

Figure 5: Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as indicated by the Color-Coded Legend Below)

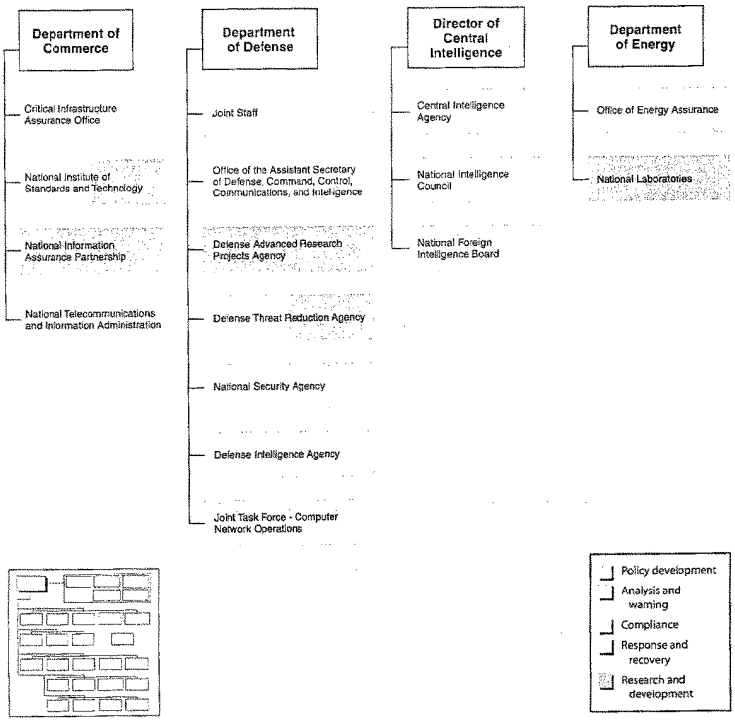


Figure 5 (cont'd): Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as Indicated by the Color-Coded Legend Below)

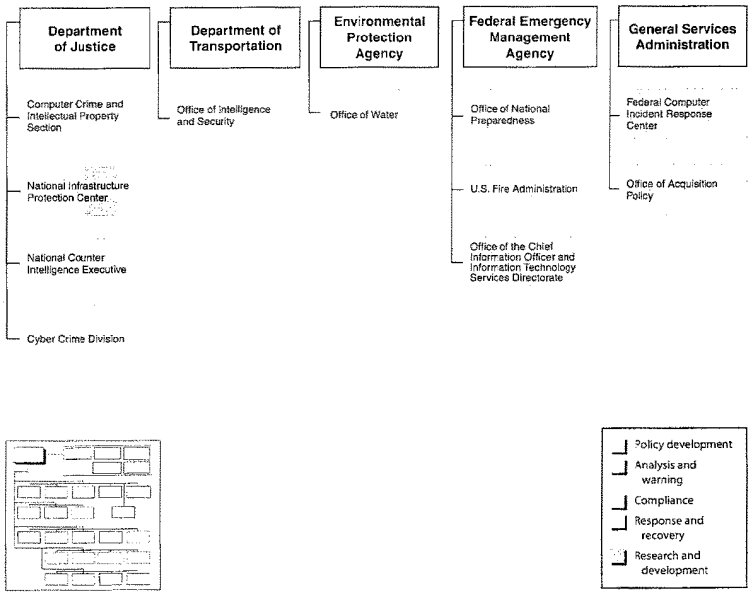
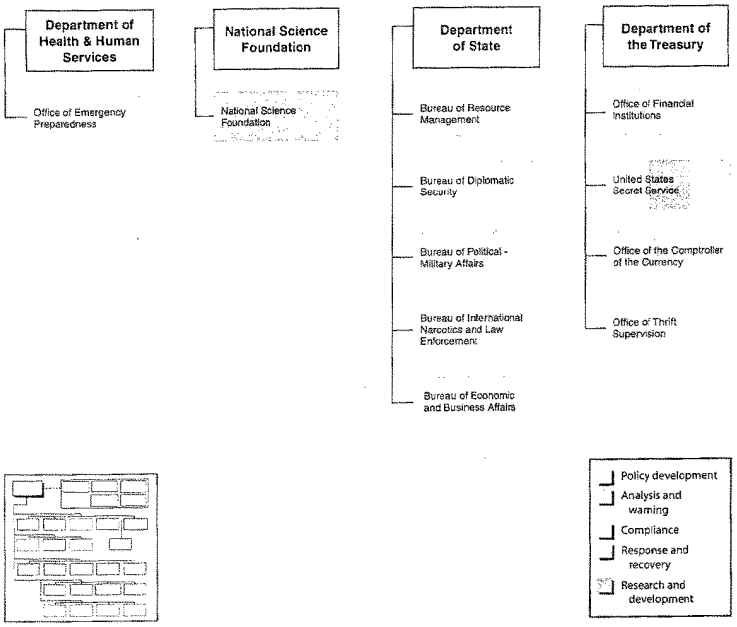


Figure 5 (cont'd): Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as indicated by the Color-Coded Legend Below)



Appendix II

Components of Executive Departments or Agencies and their Primary Activities Related to Cyber CIP

Table 2: Executive Department or Agency Components and their Primary Activities Related to Cyber CIP

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
Federal Advisory Committees					
National Infrastructure Advisory Council	√				
President's Council of Advisors on Science and Technology	√				
President's National Security Telecommunications Advisory Committee	√				
President's Information Technology Advisory Committee					
National Science and Technology Council	√				
Executive Office of the President					
Office of Homeland Security	√				
National Security Council	√				
Office of Science and Technology Policy	√			√	
National Communications System	√	√		√	
National Economic Council	√				
Office of Management and Budget	√				
President's Critical Infrastructure Protection Board	√				
Chief Information Officers Council	√				
Federal Communications Commission	√		√		
U.S. Department of Commerce					
Critical Infrastructure Assurance Office	√				
National Institute of Standards and Technology	√				√
National Information Assurance Partnership					√

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
National Telecommunications and Information Administration	√				
U.S. Department of Defense					
Joint Staff	√				
Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence	√				
Defense Advanced Research Projects Agency					√
Defense Threat Reduction Agency		√			√
National Security Agency		√			
Defense Intelligence Agency		√			
Joint Task Force - Computer Network Operations		√			
Director of Central Intelligence					
Central Intelligence Agency		√			
National Intelligence Council		√			
National Foreign Intelligence Board		√			
U.S. Department of Energy					
Office of Energy Assurance	√	√			
National Laboratories					√
U.S. Department of Justice					
Computer Crime and Intellectual Property Section	√		√		
National Infrastructure Protection Center		√	√	√	√
National Counter Intelligence Executive	√	√			
Cyber Crime Division			√		
U.S. Department of Transportation					
Office of Intelligence and Security	√				

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
Environmental Protection Agency					
Office of Water	√	√		√	
Federal Emergency Management Agency					
Office of National Preparedness	√				
United States Fire Administration	√				
Office of the Chief Information Officer and Information Technology Services Directorate	√				
U.S. General Services Administration					
Federal Computer Incident Response Center		√			
Office of Acquisition Policy	√				
Department of Health and Human Services					
Office of Emergency Preparedness				√	
National Science Foundation					√
U.S. Department of State					
Bureau of Resource Management	√				
Bureau of Diplomatic Security		√	√		
Bureau of Political-Military Affairs	√				
Bureau of International Narcotics and Law Enforcement			√		
Bureau of Economic and Business Affairs	√				
U.S. Department of Treasury					
Office of Financial Institutions	√				
United States Secret Service	√		√		√
Office of the Comptroller of the Currency	√		√		
Office of Thrift Supervision			√		

Appendix III
Related GAO Products Issued Since Fiscal Year 1996

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems. GAO-02-474. Washington, D.C.: July 15, 2002.

FDIC Information Security: Improvements Made But Weaknesses Remain. GAO-02-689. Washington, D.C.: July 15, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Information Security: Corps of Engineers Making Improvements, but Weaknesses Continue. GAO-02-589. Washington, D.C.: June 10, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Information Security: Comments on the Proposed Federal Information Security Management Act of 2002. GAO-02-677T. Washington, D.C.: May 2, 2002.

Information Security: Additional Actions Needed to Fully Implement Reform Legislation. GAO-02-407. Washington, D.C.: May 2, 2002.

Information Security: Subcommittee Post-Hearing Questions Concerning the Additional Actions Needed to Implement Reform Legislation. GAO-02-649R. Washington, D.C.: April 16, 2002.

Information Security: Additional Actions Needed to Implement Reform Legislation. GAO-02-470T. Washington, D.C.: March 6, 2002.

Financial Management Service: Significant Weaknesses in Computer Controls Continue. GAO-02-317. Washington, D.C.: January 31, 2002.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO-02-266R. Washington, D.C.: December 10, 2001.

Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-02-231T. Washington, D.C.: November 9, 2001.

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection. GAO-02-24. Washington, D.C.: October 15, 2001.

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately-Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C.: September 26, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO-01-1131R. Washington, D.C.: September 13, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T. Washington, D.C.: September 12, 2001.

Education Information Security: Improvements Made But Control Weaknesses Remain. GAO-01-1067. Washington, D.C.: September 12, 2001.

Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures. GAO-01-1073T. Washington, D.C.: August 29, 2001.

Nuclear Security: DOE Needs to Improve Control Over Classified Information. GAO-01-806. Washington, D.C.: August 24, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-751. Washington, D.C.: August 13, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-1004T. Washington, D.C.: August 3, 2001.

Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security. GAO-01-863. Washington, D.C.: July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-1005T. Washington, D.C.: July 25, 2001.

Information Security: Weak Controls Place Interior's Financial and Other Data at Risk. GAO-01-615. Washington, D.C.: July 3, 2001.

Critical Infrastructure Protection: NIPC Faces Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-769T. Washington, D.C.: May 22, 2001.

Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and HHS Would Enhance Health Data Sharing. GAO-01-459. Washington, D.C.: April 30, 2001.

Internet Privacy: Implementation of Federal Guidance for Agency Use of "Cookies." GAO-01-424. Washington, D.C.: April 27, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. GAO-01-323. Washington, D.C.: April 25, 2001.

Computer Security: Weaknesses Continue To Place Critical Federal Operations And Assets At Risk. GAO-01-500T. Washington, D.C.: April 5, 2001.

VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist. GAO-01-550T. Washington, D.C.: April 4, 2001.

Internal Revenue Service: 2001 Tax Filing Season, Systems Modernization, and Security of Electronic Filing. GAO-01-595T. Washington, D.C.: April 3, 2001.

Internal Revenue Service: Progress Continues But Serious Management Challenges Remain. GAO-01-562T. Washington, D.C.: April 2, 2001.

Information Security: Safeguarding of Data in Excessed Department of Energy Computers. GAO-01-469. Washington, D.C.: March 29, 2001.

U.S. Government Financial Statements: FY 2000 Reporting Underscores the Need to Accelerate Federal Financial Management Reform. GAO-01-570T. Washington, D.C.: March 30,2001.

Information Security: Challenges to Improving DOD's Incident Response Capabilities. GAO-01-341. Washington, D.C.: March 29, 2001.

Information Security: Progress and Challenges to an Effective Defense-Wide Information Assurance Program. GAO-01-307. Washington, D.C.: March 30, 2001.

Information Security: IRS Electronic Filing Systems. GAO-01-306. Washington, D.C.: February 16, 2001.

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. GAO-01-277. Washington, D.C.: February 26, 2001.

Information Security: Weak Controls Place DC Highway Trust Fund and Other Data at Risk. GAO-01-155. Washington, D.C.: January 31, 2001.

High Risk Series: An Update. GAO-01-263. Washington, D.C.: January 2001.

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171. Washington, D.C.: December 6, 2000.

Financial Management: Significant Weaknesses in Corps of Engineers' Computer Controls. GAO-01-89. Washington, D.C.: October 11, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T-AIMD-00-330. Washington, D.C.: September 27, 2000.

Financial Management Service: Significant Weaknesses in Computer Controls. GAO/AIMD-00-305. Washington, D.C.: September 26, 2000.

VA Information Technology: Progress Continues Although Vulnerabilities Remain. GAO/T-AIMD-00-321. Washington, D.C.: September 21, 2000.

Electronic Government: Government Paperwork Elimination Act Presents Challenges for Agencies. GAO/AIMD-00-282. Washington, D.C.: September 15, 2000.

Year 2000 Computer Challenge: Lessons Learned Can Be Applied to Other Management Challenges. GAO/AIMD-00-290. Washington, D.C.: September 12, 2000.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. GAO/AIMD-00-232. Washington, D.C.: September 8, 2000.

Computer Security: Critical Federal Operations and Assets Remain at Risk. GAO/T-AIMD-00-314. Washington, D.C.: September 11, 2000.

Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies. GAO/AIMD-00-295. Washington, D.C.: September 6, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. GAO/AIMD-00-252. Washington, D.C.: August 16, 2000.

Information Security: USDA Needs to Implement Its Departmentwide Information Security Plan. GAO/AIMD-00-217. Washington, D.C.: August 10, 2000.

Information Technology: Selected Agencies' Use of Commercial Off-the-Shelf Software for Human Resources Functions. GAO/AIMD-00-270. Washington, D.C.: July 31, 2000.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-00-269. Washington, D.C.: August 9, 2000.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000.

Electronic Signature: Sanction of the Department of State's System. GAO/AIMD-00-227R. Washington, D.C.: July 10, 2000.

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. GAO/AIMD-00-215. Washington, D.C.: July 6, 2000.

Nuclear Security: Information on DOE's Requirements for Protecting and Controlling Classified Documents. GAO/T-RCED-00-247. Washington, D.C.: July 11, 2000.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-00-218. Washington, D.C.: July 7, 2000.

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. GAO/T-AIMD-00-229. Washington, D.C.: June 22, 2000.

Computer Security: FAA Is Addressing Personnel Weaknesses, but Further Action Is Required. GAO/AIMD-00-169. Washington, D.C.: May 31, 2000.

Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities. GAO/T-AIMD-00-181. Washington, D.C.: May 18, 2000.

Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements. GAO/T-AIMD-00-171. Washington, D.C.: May 10, 2000.

Information Security: Controls Over Software Changes at Federal Agencies. GAO/AIMD-00-151R. Washington, D.C.: May 4, 2000.

VA Systems Security: Information System Controls at the VA Maryland Health Care System. GAO/AIMD-00-117R. Washington, D.C.: April 19, 2000.

Federal Information Security: Action Needed to Address Widespread Weaknesses. GAO/T-AIMD-00-135. Washington, D.C.: March 29, 2000.

Export Controls: National Security Risks and Revisions to Controls on Computer Systems. GAO/T-NSIAD-00-139. Washington, D.C.: March 23, 2000.

Financial Management: USDA Faces Major Financial Management Challenges. GAO/T-AIMD-00-115. Washington, D.C.: March 21, 2000.

Information Security: Comments on Proposed Government Information Security Act of 1999. GAO/T-AIMD-00-107. Washington, D.C.: March 2, 2000.

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. GAO/T-AIMD-00-97. Washington, D.C.: February 17, 2000.

Computer Security: Reported Appropriations and Obligations for Four Major Initiatives. GAO/AIMD-00-92R. Washington, D.C.: February 28, 2000.

Critical Infrastructure Protection: National Plan for Information Systems Protection. GAO/AIMD-00-90R. Washington, D.C.: February 11, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. GAO/T-AIMD-00-72. Washington, D.C.: February 01, 2000.

Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software. GAO/AIMD-00-55. Washington, D.C.: December 23, 1999.

Information Security: Responses to Posthearing Questions. GAO/AIMD-00-46R. Washington, D.C.: November 30, 1999. Sen. Judiciary Committee.

Information Security Risk Assessment: Practice of Leading Organizations (A supplement to GAO's May 1998 Executive Guide on Information Security Management.) GAO/AIMD-00-33. Washington, D.C.: November 1999.

Information Security: Weaknesses at 22 Agencies. GAO/AIMD-00-32R. Washington, D.C.: November 10, 1999.

Information Security: SSA's Computer Intrusion Detection Capabilities. GAO/AIMD-00-16R. Washington, D.C.: October 27, 1999.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. GAO/T-AIMD-00-7. Washington, D.C.: October 6, 1999.

Financial Management Service: Significant Weaknesses in Computer Controls. GAO/AIMD-00-4, Oct. 4, 1999.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. GAO/AIMD-00-5. Washington, D.C.: October 4, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. GAO/AIMD-00-1. Washington, D.C.: October 1, 1999.

Information Security: The Proposed Computer Security Enhancement Act of 1999. GAO/T-AIMD-99-302. Washington, D.C.: September 30, 1999.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-99-280. Washington, D.C.: September 15, 1999.

Information Security: NRC's Computer Intrusion Detection Capabilities. GAO/AIMD-99-273R. Washington, D.C.: August 27, 1999.

DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk. GAO/AIMD-99-107. Washington, D.C.: August 26, 1999.

Battlefield Automation: Opportunities to Improve the Army's Information Protection Effort. GAO/NSIAD-99-166. Washington, D.C.: August 11, 1999.

Information Security: Answers to Posthearing Questions. GAO/AIMD-99-272R. Washington, D.C.: August 9, 1999.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-99-242. Washington, D.C.: August 6, 1999.

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-99-227. Washington, D.C.: July 30, 1999.

Medicare: Improvements Needed to Enhance Protection of Confidential Health Information. HEHS-99-140. Washington, D.C.: July 20, 1999.

Medicare: HCFA Needs to Better Protect Beneficiaries' Confidential Health Information. GAO/T-HEHS-99-172. Washington, D.C.: July 20, 1999.

Information Security: Recent Attacks on Federal Web Sites Underscore Need for Strengthened Information Security Management. GAO/T-AIMD-99-223. Washington, D.C.: June 24, 1999.

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls. GAO/AIMD-99-161. Washington, D.C.: June 8, 1999.

Information Security: Many NASA Mission-Critical Systems Face Serious Risks. GAO/AIMD-99-47. Washington, D.C.: May 20, 1999.

Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data. GAO/T-AIMD-99-146. Washington, D.C.: April 15, 1999.

Financial Audit: 1998 Financial Report of the United States Government. GAO/AIMD-99-130. Washington, D.C.: March 31, 1999.

Securities Fraud: The Internet Poses Challenges to Regulators and Investors. GAO/T-GGD-99-34. Washington, D.C.: March 22, 1999.

IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk. GAO/AIMD-99-38. Washington, D.C.: December 14, 1998.

Financial Management Service: Areas for Improvement in Computer Controls. GAO/AIMD-99-10. Washington, D.C.: October 20, 1998.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-99-6. Washington, D.C.: October 14, 1998.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-99-2. Washington, D.C.: October 14, 1998.

Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls. GAO/AIMD-98-274. Washington, D.C.: September 28, 1998.

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk. GAO/AIMD-98-92. Washington, D.C.: September 23, 1998.

Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets. GAO/T-AIMD-98-312. Washington, D.C.: September 23, 1998.

VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure. GAO/AIMD-98-175. Washington, D.C.: September 23, 1998.

Defense Information Superiority: Progress Made, but Significant Challenges Remain. GAO/NSIAD/AIMD-98-257. Washington, D.C.: August 31, 1998.

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems. GAO/T-AIMD-98-251. Washington, D.C.: August 6, 1998.

Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk. GAO/T-AIMD-98-170. Washington, D.C.: May 19, 1998.

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations. GAO/AIMD-98-145. Washington, D.C.: May 18, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD-98-155. Washington, D.C.: May 18, 1998.

Executive Guide: Information Security Management: Learning From Leading Organizations. GAO/AIMD-98-68. Washington, D.C.: May 1998.

U.S. Government Financial Statements: Results of GAO's Fiscal Year 1997 Audit. GAO/T-AIMD-98-128. Washington, D.C.: April. 1, 1998.

Financial Audit: 1997 Consolidated Financial Statements of the United States Government. GAO/AIMD-98-127. Washington, D.C.: March 31, 1998.

Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements. GAO/AIMD-98-18. Washington, D.C.: December 24, 1997.

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls. GAO/AIMD-97-128. Washington, D.C.: September 9, 1997.

Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements. GAO/AIMD-97-89. Washington, D.C.: July 31, 1997.

Small Business Administration: Better Planning and Controls Needed for Information Systems. GAO/AIMD-97-94. Washington, D.C.: June 27, 1997.

Social Security Administration: Internet Access to Personal Earnings and Benefits Information. GAO/T-AIMD/HEHS-97-123. Washington, D.C.: May 6, 1997.

Budget Process: Comments on S.261–Biennial Budgeting and Appropriations Act. GAO/T-AIMD-97-84.

IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified. GAO/T-AIMD-97-82. Washington, D.C.: April 15, 1997.

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses. GAO/T-AIMD-97-76. Washington, D.C.: April 10, 1997.

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses. GAO/AIMD-97-49. Washington, D.C.: April 8, 1997.

High Risk Series: Information Management and Technology. GAO/HR-97-9, Feb. 1997.

Information Security: Opportunities for Improved OMB Oversight of Agency Practices. GAO/AIMD-96-110. Washington, D.C.: September 24, 1996.

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements. GAO/AIMD-96-101. Washington, D.C.: July 11, 1996.

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses. GAO/AIMD-96-106. Washington, D.C.: June 7, 1996.

Information Security: Computer Hacker Information Available on the Internet. GAO/T-AIMD-96-108. Washington, D.C.: June 5, 1996.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84. Washington, D.C.: May 22, 1996.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/T-AIMD-96-92. Washington, D.C.: May 22, 1996.

Security Weaknesses at IRS' Cyberfile Data Center. GAO/AIMD-96-85R. Washington, D.C.: May 9, 1996.

Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome to Achieve Success. GAO/T-AIMD-96-75. Washington, D.C.: March 26, 1996.

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1994 and 1993. GAO/AIMD-96-22. Washington, D.C.: February 26, 1996.

Financial Management: General Computer Controls at the Senate Computer Center. GAO/AIMD-96-15. Washington, D.C.: December 22, 1995.

Financial Management: Challenges Facing DOD in Meeting the Goals of the Chief Financial Officers Act. GAO/T-AIMD-96-1. Washington, D.C.: November 14, 1995.

(310163)

Mr. HORN. Thank you. We appreciate that.

Our next presenter is Ronald L. Dick, the Director of the National Infrastructure Protection Center, Federal Bureau of Investigation. I want to express the feelings of the Committee on Government Reform and this subcommittee in particular about what you have done to help us in many ways, and so thank you very much, Mr. Dick. You do a fine job down there.

STATEMENT OF RONALD L. DICK, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Mr. DICK. Thank you, Mr. Chairman, for this opportunity to discuss our government's important and continuing challenges with respect to critical infrastructure protection. But before I begin my statement I would like to express my appreciation to you for your service in the House and note that everyone concerned with infrastructure protection will miss your leadership.

Mr. HORN. That is kind of you.

Mr. DICK. Thank you, sir.

And ITC representatives have testified several times in front of this committee, most recently in September of last year. Since that time, while the Nation has focused on the war against terrorism, the NIPC has forged ahead on several fronts.

I have been asked many times about what keeps me up at night and I think about a scenario that combines a serious physical attack with a concurrent cyber attack which would tie up 911 systems or stop the flow of electricity and water during the crisis. We work to prevent such a scenario through two-way information sharing. Because approximately 85 percent of the Nation's critical infrastructures are owned by the private sector, we rely heavily on private sector information sharing.

In the written statement, I discuss some of the challenges we must overcome in two-way information sharing. I will focus on two areas in which we have made substantial progress in the last year.

First, we have built many trusting relationships with members of the private sector, particularly those through our government-private sector infrastructure protection partnership, known as InfraGard, and with information sharing and analysis centers. For example, InfraGard membership has grown by more than 600 percent in the last 14 months from 800 to nearly 5,000.

Second, our news unit, the ISAC's Support and Development Unit, was designed to assist in the development and expansion of ISACs. Since formation of that unit, information sharing agreements have been signed with ISACs for telecommunications, information technology, food, water supply, emergency services like fire, banking and finance, chemical sectors and the Aviation Administration. Tomorrow I am scheduled to sign another agreement, adding the National Association of State Chief Information Officers to our list of infrastructure protection partners.

One of the most recent agreements was with the ISAC for fire emergency services led by the U.S. Fire Administration, an organization which has been a model for mutual benefits of two-way information sharing. Since that agreement, we have shared intelligence on scuba diving threats to waterfront facilities, suspicious

attempts to purchase an ambulance in New York and the theft of a truck with 10 tons of cyanide in Mexico. In turn, they have told us of suspicious foreign nationals attempting to gather information on emergency services.

However, more work still needs to be done. The annual Computer Security Institute and FBI Computer Crime and Security Survey, released in April, indicated that 90 percent of the respondents detected computer security breaches in the last 12 months. Only 34 percent reported the intrusion to law enforcement. On the positive side, that 34 percent is more than double the 16 percent who reported intrusions in 1996. This nonreporting impairs the government's ability to analyze threats and vulnerabilities and take appropriate action. The two primary reasons for not reporting were the fear of negative publicity and the belief that competitors would use the information against them if it were released.

First, I assure you that the Department of Justice and the FBI, Office of General Counsel will be happy to discuss with your staffs the issues more thoroughly regarding information sharing because it always must be kept in mind that sharing of information is voluntary. Therefore, it becomes the government's burden to demonstrate it can and will protect information.

One of the issues we have heard for years is that companies are concerned that information they provide to the government will be released by the government under the Freedom of Information Act. We looked at the Freedom of Information Act and discussed it with the private sector. Under exemption (b)(4) of FOIA, the government is not required to disclose, "trade secrets and commercial or financial information obtained from a person and privileged or confidential."

On the face of that statute, you find the definite—you don't find, rather, the definition of those key terms. Companies asked us what "trade secrets" meant under FOIA as well as the scope and terms of information. They asked, for example, is vulnerability information considered commercial or financial? They also asked whether under the statute information gets different protection if it is voluntarily provided to the government.

We worked with the Department of Justice and also did our own legal research. In doing so, we found a number of important cases that discuss these issues. The most important, I am told, is a case decided by the D.C. District Circuit Court of Appeals called Critical Mass Energy Project vs. the Nuclear Regulatory Commission. Nonetheless, despite these cases and some others like it, companies want clear statutes with straightforward language. They do not want to be kept up to date on the latest cases or have to keep up to date on the latest cases. They want a simple statute they can understand. Without that, many companies will not share information.

The question of whether in the abstract we can protect the information becomes meaningless if the companies will not give us the information in the first place. Many companies seek certain outcomes and they don't want to rely on a judge's decision. They also don't want to face even the possibility of having to go to court to litigate the protection of their information whether under FOIA or under the Trade Secrets Act. Finally, they are also concerned about

the State open records laws. Many have told us that they want to be able to share sensitive information with the Federal Government and they would like the Federal Government to be able to share information with them and would like to be able to share information with the States. But they are equally clear that if the sensitive information becomes public, they will not share it. Sharing a lot of this information publicly would weaken the Nation's security, not strengthen it.

The NIPC has been asked to engage in a constructive dialog with industry in order to promote information sharing. For over 4 years we have heard this same message. We would like the FOIA issue resolved in a manner that industry is convinced of the government's ability to protect their information.

At a recent Senate hearing before Senator Lieberman, the NIPC, myself and the Department of Justice committed to work with Congress on these concerns so as to resolve them.

And let me conclude. Faced with the hard fact that most companies are not reporting, the NIPC has promoted an aggressive outreach program and is seeing results. The system of information sharing amongst ISACs, the NIPC, government agencies and the private sector is beginning to work. At the NIPC we continue to seek partnerships and means which promote two-way information sharing. As Director Mueller stated in a speech on July 16, prevention of terrorist attacks is by far and away our most urgent priority. We can only prevent attacks on our critical infrastructures by building an intelligence base, analyzing that information and providing timely, actionable, threat-related products to our private and public sector partners.

Therefore, we will continue our efforts with your committee in improving information sharing and infrastructure protection, and I welcome your comments.

[The prepared statement of Mr. Dick follows:]

Statement for the Record of Ronald L. Dick,
Director, National Infrastructure Protection Center,

Federal Bureau of Investigation
Before the
House Committee on Governmental Reform,
Government Efficiency, Financial Management and
Intergovernmental Relations Subcommittee

July 24, 2002

Mr. Chairman and members of the Subcommittee, thank you for inviting me here today to testify on the topic, "Cyber Terrorism and Critical Infrastructure Protection." Holding this hearing demonstrates your individual commitment to improving the security of our Nation's critical infrastructures and this Committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. We have seen how a terrorist attack can have immediate simultaneous impact on several interdependent infrastructures. The terrorist attacks in New York directly and seriously affected banking and finance, telecommunications, emergency services, air and rail transportation, energy and water supply. My testimony today will address the improvement of infrastructure protection through two-way information sharing and the challenges we face in the future.

Since our last testimony before this Subcommittee on September 26, 2001, the National Infrastructure Protection Center has seen increases in personnel, funding, and interagency participation, allowing us to make great progress in accomplishing our mission. As set forth in Presidential Decision Directive 63 (PDD-63), the mission of the NIPC is to provide "a national focal point for gathering information on threats to the infrastructures" and to provide "the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." The Directive defines critical infrastructures to include "those physical and cyber-based systems essential to the minimum operations of the economy and government," to include, without limitation, "telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." Our combined mission supports information and physical security, law enforcement, national security, and the military.

To accomplish this mission, we have had to build a coalition of trust amongst all government agencies, between the government and the private sector, amongst the different business interests within the private sector itself, and in concert with the greater international community. We have begun to earn that trust, and two-way information sharing has increased considerably since our last testimony here.

OUTREACH EFFORTS

To better share information, the NIPC has spearheaded an aggressive outreach effort.

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

CRITICAL NEED FOR OUTREACH

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

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

The InfraGard program is a nationwide initiative that grew out of a pilot program started at the Cleveland FBI field office in 1996. Today, all 56 FBI field offices have active InfraGard chapters. Nationally, InfraGard has over 5000 members. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service the FBI provides to InfraGard members free of charge. It particularly benefits small businesses which have nowhere else to turn for assistance. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The InfraGard program received the 2001 World Safe Internet Safety Award from the Safe America Foundation for its efforts.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. InfraGard

provides a mechanism for the public and private sectors to exchange information pertaining to cyber intrusion matters, computer network vulnerabilities and physical threats on infrastructures. All InfraGard participants are committed to the proposition that the exchange of information about threats on these critical infrastructures is an important element for successful infrastructure protection efforts. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

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

InfraGard is responsible for providing four basic services to its members: secure and public WebSites, an alert and incident reporting network, local chapter activities, and a help desk. Under this program the FBI provides a secure electronic communications capability to all InfraGard members so that the NIPC can provide threat information to private industry owners and operators, and encourage private industry coordination with law enforcement, and each other, on cyber and related physical incidents. This will be accomplished by expanding the established separate WebSite and electronic mail system. The program anticipates approximately 4,000 new members expected in calendar year 2002. A number of the larger field divisions have initiated additional chapters in larger cities located in their respective geographic area of responsibility. The warnings that are provided to our InfraGard members improve the relationship between private industry and the local FBI offices due to the increased level of trust that is often established. It should be noted that the InfraGard program is not responsible for producing NIPC's alerts and warnings. These alerts and warnings are produced and disseminated by NIPC's Analysis and Warning Section.

Information Sharing and Analysis Centers (ISACs)

The NIPC has recently initiated the establishment of an Information Sharing and Analysis Center (ISAC) Support and Development Unit, whose mission is to enhance private sector cooperation and trust, resulting in two-way sharing of information and increased security for the nation's critical infrastructures. The ISAC Development and Support Unit has assigned personnel to each ISAC to serve as NIPC's liaison to that sector. When an ISAC receives information from a member, they forward the information to their NIPC liaison, who then works with NIPC's Analysis and Information Sharing Unit and Watch and Warning Unit to coordinate an appropriate response. The NIPC now has information sharing agreements with nine ISACs, including those representing energy, telecommunications, information technology, banking and finance, emergency law enforcement,

emergency fire services, water supply, food, and chemical sectors. Several more agreements are in the final stages, including one to be signed on July 25th with the National Association of State Chief Information Officers. Just as important, the NIPC is receiving reports from member companies of the ISACs. The NIPC has proven to these companies that it can properly safeguard their information and can provide them with useful information. It is because of such reporting that NIPC's products are improving.

Three examples bear discussion. The North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC for an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information and the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. Additionally, some information available to the NIPC may be classified or law enforcement sensitive and, thus, unavailable to many in the industry. A group of NERC officials have been granted security clearances in order to access classified material on a need-to-know basis. Once the NIPC has determined that a warning should be issued, cleared electric power experts will be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide members of the industry with unclassified, nonproprietary, timely and actionable information to the maximum extent possible.

One of our most recent agreements was with the ISAC for Emergency Services - Fire, the U.S. Fire Administration, an organization which has been a model for the mutual benefits of two-way information sharing. Since that agreement, we have shared intelligence on diver threats to waterfront facilities, suspicious attempts to purchase an ambulance in New York, and the theft of a truck with 10 tons of cyanide in Mexico. In turn, they have told us of suspicious foreign nationals visiting fire stations to gather information and of foreign nationals calling fire and EMS departments and visiting their web sites to gather information on capabilities, watch schedules and manning levels. Such two-way information sharing provides significant safety and infrastructure protection benefits to the public we serve.

The telecommunications ISAC provides a good example of positive, two-way information sharing. In his July 9, 2002 testimony before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, Bill Smith, Chief Technology Officer, BellSouth Corporation, stated: "With respect to FOIA (Freedom of Information Act), many companies are hesitant to voluntarily share sensitive information with the government because of the possible release of this information to the public." He further noted that BellSouth does share information with the Telecommunications ISAC, but it is "done on a limited basis, within trusted circles, and strictly

within a fashion that will eliminate any liability or harm from FOIA requests for BellSouth information." He adds that BellSouth has benefitted from advance warnings of worms and viruses. The telecommunications ISAC provided BellSouth with their first notification of the NIMDA worm, resulting in the successful defense of their networks. BellSouth, in turn, was the first to notify the ISAC of problems associated with the simple network management protocol. Although this is an example of two-way information sharing, it is also an example of reluctant sharing resulting from legal, economic and trust barriers. Smith goes on to list BellSouth's concerns about information sharing, including: "liability under the Freedom of Information Act, third-party liability (e.g., sharing suspected problems about a piece of equipment before thoroughly tested and verified), the lack of a defined antitrust exemption for appropriate information sharing concerning infrastructure vulnerabilities, possible disclosure of information under state sunshine laws, disclosure of sensitive corporate information to competitors, declassification of threat/intelligence information to a level that can be acted upon by company personnel, and the natural inclination of law enforcement, DoD, and intelligence agencies to dissuade the sharing of information related to criminal investigations."

The NIPC routinely shares information with the public and private sectors to help them better protect themselves. That does not mean that information is broadcast across the news media in every instance. While public statements are the best alternative in some cases, in other cases the NIPC has approached victim companies as to a specific investigation, and Information Sharing and Analysis Centers (ISACs) or government agencies privately to help evaluate uncorroborated information in order then to provide public comment. In many cases, a tiered approach is taken so that information with the appropriate level of detail is pushed to the right audiences. If the NIPC finds that despite issuing an advisory, a widespread problem persists or grows, then we will raise the volume, and a more public advisory will be issued to reach a wider audience.

NIPC INFORMATION SHARING PRODUCTS

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

(for example, because they reflect non-public sources and methods), it attempts to issue most reports at the unclassified level and to the widest audience possible.

WATCH AND WARNING

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

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

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

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

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

Since its inception, the NIPC has issued over 120 warning products. A number of warning products have preceded incidents or prevented them entirely by alerting the user community to a new vulnerability or hacker exploit before acts are committed or exploits are used on a widespread basis. The Center has had particular success in alerting the user community to the presence of Denial of Service tools on the network and has in some cases provided a means to discover the presence of tools on a network.

The NIPC is integrated into national level warning systems both through structures established by the National Security Council and by other agencies. Of particular note is the fact that the NIPC has been fully engaged in the planning and implementation of the interagency Cyber Warning Information Network (CWIN) a network through which the watch centers from FedCIRC, NSA, JTF-CNO, National Communications System (NCS) and NIPC exchange information daily.

INTRA-GOVERNMENT INFORMATION SHARING

PDD-63 mandates that government agencies will share information with the NIPC. The NIPC has established effective information sharing relationships across the U.S. Government. These arrangements are not always codified in formal interagency agreements or Memoranda of Understanding, but the important point is that they are working.

The NIPC has formed an Interagency Coordination Cell (IACC) at the Center which holds monthly meetings regarding ongoing investigations. To date, the IACC's growing membership has risen to approximately 35 government agencies that meet on a monthly basis, and as needed, to address specific threats and vulnerabilities. The IACC include representation from NASA , U.S. Postal Service, Air Force Office of Special Investigations (AFOSI), U.S. Secret Service, U.S. Customs, Departments of Energy, State and Education, and the Central Intelligence Agency, to name a few.

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

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

The Department of Defense has the second largest (after FBI) interagency contingent in the NIPC. The Deputy Director of the NIPC is a two-star Navy Rear Admiral; the Executive Director is detailed from the Air Force Office of Special Investigations; the head of the NIPC Watch is a Naval Reserve officer; and the head of the Analysis and Information Sharing Unit is a National Security

Agency detailee. There are also liaison representatives from the National Imagery and Mapping Agency and the Joint Programs Office. A contingent of DoD reservists serves in the Center to provide additional critical infrastructure expertise and emergency surge capabilities. NIPC works particularly closely with the DoD through liaison with the Joint Task Force-Computer Network Operations (JTF-CNO). NIPC members stay in close contact with their JTF-CNO counterparts, providing mutual assistance on intrusion cases into DoD systems, as well as on other matters. NIPC alerts, advisories, and assessments are routinely coordinated with the JTF-CNO prior to release to solicit JTF input. On several occasions, the NIPC and JTF-CNO have coordinated and issued joint cyber warnings on the same matter. There is also significant interaction with the military services, the Joint Staff, the Office of the Secretary, and other major DoD agencies.

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

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

More recently, in October of 2001, President Bush issued Executive Order 13231, which establishes the President's Critical Infrastructure Protection Board to "recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems." EO 13231 expressed the current Administration's continued support of the NIPC's mission under PDD 63 and distinguishes the interagency entity from any particular Department by separately designating the Director of the NIPC to serve as a member of the newly created President's Board. The President also designated the Director of the NIPC to serve on the Board's Coordination Committee, and recognized the NIPC's significant roles in, among other things, outreach to the private sector and state and local governments, as well as in the area of information sharing.

Since 1998, the NIPC has been developing the FBI's Key Asset Initiative, to identify those entities that are vital to our national security, including our economic well-being. The information

is maintained to support the broader effort to protect the critical infrastructures against both physical and cyber threats. This initiative benefits national security planning efforts by providing a better understanding of the location, importance, contact information and crisis management for critical infrastructure assets across the country. We have worked with the DoD and the Critical Infrastructure Assurance Office (CIAO) in this regard.

FEDERAL, STATE AND LOCAL INFORMATION SHARING

Emergency Law Enforcement Services Sector

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

State Infrastructure Protection Center (SIPC) efforts

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

FEDERAL GOVERNMENT AND THE PRIVATE SECTOR

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

The NIPC and the Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Mellon University have formed a mutually beneficial contractual relationship. The NIPC receives information from the CERT (including advance Special Communications about

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

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT AND INTERNATIONAL PARTNERS

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

On the information infrastructure side of the equation, a typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Even intrusions into U.S. systems by a perpetrator operating within the U.S. often require international investigative activity because the attack is routed through Internet Service Providers and computer networks located outside the United States. When evidence is located within the United States, the NIPC coordinates law enforcement efforts which might include: subpoenaing records by FBI agents, conduct of electronic surveillance, execution of search warrants, seizing and examining of evidence. We can not do those things ourselves to solve a U.S. criminal case overseas. Instead, we must depend on the local authorities to assist us. This means that effective international cooperation is essential to our ability to investigate cyber crime. The FBI's Legal Attaches (LEGATs) provide the means to accomplish our law enforcement coordination abroad, and are often the first officials contacted by foreign law enforcement should an incident occur overseas that requires U. S. assistance. NIPC personnel are in almost daily contact with LEGATs around the world to assist in coordinating requests for information.

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

case in international matters, because electronic evidence is fleeting and, if not secured quickly, can be lost forever.

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

DEPARTMENT OF HOMELAND SECURITY

Homeland Security legislation currently being considered calls for certain NIPC functions relating to watch and warning, and private sector outreach to be transferred consistent with the new department's overall mission. The operational remainder of NIPC, including the field investigative functions, will remain at the FBI, under the new Cyber Division.

CONCLUSION

At the NIPC we continue to seek partnerships which promote two-way information sharing. As Director Mueller stated in a speech on July 16th, "Prevention of terrorist attacks is by far and away our most urgent priority." We can only prevent attacks on our critical infrastructures by building an intelligence base, analyzing that information, and providing timely, actionable threat-related products to our public and private sector partners. We welcome the efforts of your Committee in improving information sharing, and I look forward to addressing any questions you might have.

Mr. HORN. Thank you very much. We will now hear from John S. Tritak, Director of the Critical Infrastructure Assurance Office in the Department of Commerce. Now that is partly, with NIST, also involved in standards and that kind of thing. Very good, if you want to give us a better view of that, start in with it.

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

Mr. TRITAK. Thank you for the opportunity to be here today. I submitted my written remarks, and I would be more than happy to talk about the move to the Department of Homeland Security and our respective roles as you would like, but I would like to touch on a few themes that have arisen during the course of this hearing and give some reflection on those in my brief remarks now.

I want to begin by focusing—homeland security differs fundamentally from what I would call classic national security. And by classic national security, I am referring to those things the government more or less did on its own on behalf of the United States and its citizenry. We are now confronted with a unique challenge. And that is because, as we have heard from al Qaeda and others, is that the terrorists have indicated that the economy is a target, particularly the pillars of that economy, and the vast majority of those are privately owned and operated. Terrorists' followers have been urged to attack these pillars of the economy wherever vulnerabilities exist, whether they are in the physical domain or in the cyber domain.

And we know they're looking at the cyber domain as well. And we have heard a little bit earlier that attacking SCADA systems or major facilities through cyberspace is not easy and is not something that the average hacker can do, and I would completely concur in that. It is not easy, but I will submit the terrorists are not lazy. And it wasn't easy to orchestrate the hijacking of four aircraft and turn those aircraft into cruise missiles.

The point of all of these terrorist activities is to force the United States to look inward and change and rethink its global commitments overseas, particularly in the Persian Gulf and the Middle East. Their goal was to create serious impact and force us to redo and rethink our commitments overseas.

So I would submit to you it is not a question of whether cyber terrorism exists or whether it is overblown. I think to the extent that our economy relies on information systems and networks to function and to the extent there are vulnerabilities of the kind that could be exploited to cause harm in combination with other forms of attack—Ron Dick just mentioned one. I think he is right on this. We don't necessarily have to envision terrorism playing out like a war game or Nintendo. We are talking about a situation where perhaps in combination with a devastating physical attack certain key information systems networks are disrupted and therefore exacerbate an already terrible situation because that is the impact they are seeking. It is their goal we have to keep an eye on when we are talking about this problem. Therefore, because the economy is largely privately owned and operated, we have to see homeland security as a shared responsibility, and this is going to require redefining our respective roles between government and industry and

how we go about achieving this new goal, and that is going to require a level of collaboration that frankly we've never had to have before.

And that is why I think it is very important when we create this new department that the culture of partnership and collaboration suffuse that organization. It has to actually build on the premise that government and industry together need to achieve this goal and that neither government nor industry alone can do it.

Information sharing is deemed one very important way in which we actually operationalize homeland security, and information sharing is taking place now. Ron Dick will tell you and many of the ISAC people will tell you they are sharing now. But the real goal here is to create an environment where dynamic sharing can take place on an ongoing basis to deal with problems as they arise in real-time. And I would submit to you that the question with respect to FOIA or any other question is whether the current statutory and regulatory environment is conducive to promoting voluntary acts of information sharing.

Now, this is not an easy issue and I know there are very important public interests and public goods at stake here and honest people can disagree over the challenge of open government on the one hand and the need to secure information and how it could come into conflict. And frankly, it is the Congress who is going to have to resolve these problems.

I also want to make clear that any change in the FOIA is not going to be a silver bullet because the one thing you can't do through the regulation or statutory reform is create trust and legislate trust. That has to come out of experience. What I would suggest, however, is that to the extent that the current environment is viewed as an impediment that we very carefully narrow reform to actually create an environment that induces that collaboration and that kind of dynamic information sharing which I think everyone agrees needs to take place if we are going to achieve the mission of securing our homeland.

And I thank you for the opportunity to be here, Mr. Chairman. You will be deeply missed by all of us who have respected your work over these last few years.

[The prepared statement of Mr. Tritak follows:]

Statement of

John S. Tritak
Director
Critical Infrastructure Assurance Office
Bureau of Industry and Security
United States Department of Commerce

BEFORE THE
HOUSE COMMITTEE ON GOVERNMENT REFORM'S SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS
July 24, 2002

Introduction

Mr. Chairman, members of the Committee, I am honored to appear before you today to discuss cyber terrorism and the nation's critical infrastructure protection activities. I look forward to discussing with you the important role that the Critical Infrastructure Assurance Office (CIAO) plays in this environment.

As you know, the creation of the Department of Homeland Security is the most sweeping reorganization of our national security establishment in over 50 years. However, this decision was made on the basis of careful study and experience gained since September 11. The Administration considered a number of organizational approaches for the new Department proposed by various commissions, think tanks, and Members of Congress. The Secretary of Commerce, the Under Secretary and I - as well as all other senior management at the Commerce Department - fully support the President's plan and stand ready to undertake necessary efforts to facilitate the creation of the new Department as soon as possible.

The topic of this hearing – cyber security and its role in our nation's overall homeland security strategy – is a subject that I have been involved with intimately for many years. I am the Director of the Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce. In addition, I am a member of the President's Critical Infrastructure Protection Board, and I work closely with Board staff in conducting and coordinating critical infrastructure protection activities. I have spoken to the private sector and to state and local government officials on the topic of critical infrastructure assurance and cyber security on several occasions. Through these activities, I have come to appreciate the need for greater coordination of efforts to protect our homeland security including cyber security.

I would like to take this opportunity to provide some background on the CIAO and to discuss briefly some of the specific activities and initiatives we are currently undertaking on cyber security and homeland security.

What are the Components of the Nation's Critical Infrastructure?

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

These infrastructures are deemed "critical" because their incapacity or destruction could have a debilitating regional or national impact. These infrastructures relate to:

- Agriculture
- Food
- Water supply
- Public Health
- Emergency Services
- Government Services
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Banking and finance
- Transportation
- Chemical Industry
- Postal and Shipping

Critical infrastructure assurance is concerned with the readiness, reliability, and continuity of infrastructure services (which rely on physical and cyber based assets) so that they are less vulnerable to disruptions, so that any impairment is of short duration and limited in scale, and that services are readily restored when disruptions occur.

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

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

Primary Threats to Critical Infrastructure Components

Threats to critical infrastructure fall into two overlapping categories:

- Physical attacks against the "real property" components of the infrastructures; and
- Cyber attacks against the information or communications components that control these infrastructures.

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

What is new are the operational challenges to assured service delivery arising from an increased dependence on information systems and networks to operate critical infrastructures. This dependence exposes the infrastructures to new vulnerabilities.

The cyber tools needed to cause significant disruption to infrastructure operations are readily available. Within the last three years alone there has been a dramatic expansion of accessibility to the tools and techniques that can cause harm to critical infrastructures by electronic means.

One does not have to be a "cyber terrorist" or an "information warrior" to obtain and use these new weapons of mass disruption. Those who can use these tools and techniques range from the recreational hacker to the terrorist to the nation state intent on obtaining strategic advantage. From the perspective of individual enterprises, the consequences of an attack can be the same, regardless of who the attacker is. Disruptions to the delivery of vital services resulting from attacks on critical infrastructures thus pose an unprecedented risk to national and economic security. What if the recent computer viruses Code Red and Nimda had hostile payloads in them and did more than just threaten the stability, reliability and dependability of the Internet?

Securing the nation's critical infrastructures against cyber attacks presents yet another difficult problem. The Federal government cannot post soldiers or police officers at the perimeters of telecommunications facilities or electric power plants to keep out digital attackers. There are no boundaries or borders in cyberspace.

Background on the Critical Infrastructure Assurance Office

The CIAO is not a new arrival to the homeland security effort: we have been working to realize the objective of critical infrastructure assurance for four years. The CIAO was created in May 1998 by presidential directive to serve as an interagency office located at the Department of Commerce to coordinate the Federal Government's initiatives on critical infrastructure assurance.

On October 16, 2001,President Bush signed Executive Order 13231 (the Order), entitled "Critical Infrastructure Protection in the Information Age." Under the Order, the CIAO was designated a member of and an advisor to the newly created President's Critical Infrastructure Protection Board (the Board). The Board was created to coordinate Federal efforts and programs relating to the protection of information systems and networks essential to the operation of the nation's critical infrastructures. In carrying out its responsibilities, the Board fully coordinates its

efforts and programs with the Assistant to the President for Homeland Security.

Major CIAO Activities and Initiatives

CIAO's responsibilities for developing and coordinating national critical infrastructure policy focus on three key areas: (A) promoting national outreach and awareness campaigns both in the private sector and at the state and local government level; (B) assisting Federal agencies to analyze their own risk exposure and critical infrastructure dependencies; and (C) coordinating the preparation of an integrated national strategy for critical infrastructure assurance.

A. Outreach and Awareness

The Federal government acting alone cannot hope to secure our nation's critical infrastructures. The national policy of infrastructure assurance can only be achieved by a voluntary public-private partnership of unprecedented scope involving business and government at the Federal, State, and local levels. Forging a broad based partnership between industry and government lies at the heart of the CIAO's mission.

Private Sector Partnerships: CIAO has developed and implemented a nation-wide industry outreach program targeting senior corporate leadership responsible for setting company policy and allocating company resources. The challenge of such an effort is to present a compelling business case for corporate action. The primary focus of the CIAO's efforts continues to be on the critical infrastructure industries (i.e., agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, banking and finance, postal and shipping, energy, chemical industry, and transportation). The basic thrust of these efforts is to communicate the message that critical infrastructure assurance is a matter of corporate governance and risk management. Senior management is responsible for securing corporate assets - including information and information systems. Corporate boards are accountable, as part of their fiduciary duty, to provide effective oversight of the development and implementation of appropriate infrastructure security policies and best practices.

In addition to infrastructure owners and operators, the CIAO's awareness and outreach efforts also target other influential stakeholders in the economy. The risk management community - including the audit and insurance professions - is particularly effective in raising matters of corporate governance and accountability with boards and senior management. In addition, the investment community is increasingly interested in how information security practices affect shareholder value - a concern of vital interest to corporate boards and management.
In partnership with these communities, the CIAO has worked to translate potential threats to critical infrastructure into business case models that corporate boards and senior management can understand. More corporate leaders are beginning to understand that tools capable of disrupting their operations are readily available not merely to terrorists and hostile nation states but to a wide-range of potential "bad actors." As a consequence, more of them understand that that the risks to their companies can and will affect operational survivability, shareholder value, customer relations, and public confidence.

The CIAO has also worked actively to facilitate greater communication among the private

infrastructure sectors themselves. As individual Federal lead agencies formed partnerships with their respective critical infrastructure sectors, private industry representatives quickly identified a need for cross-industry dialogue and sharing of experience to improve the effectiveness and efficiency of individual sector assurance efforts. In response to that expressed need, the CIAO assisted its private sector partners in establishing the Partnership for Critical Infrastructure Security (PCIS). The PCIS provides a unique forum for government and private sector owners and operators of critical infrastructures to address issues of mutual interest and concern. It builds upon, without duplicating, the public-private efforts already being undertaken by the Federal Lead Agencies.

State and Local Government Partnerships: The CIAO has developed an outreach and awareness program for state and local governments to complement and support its outreach program to industry. State and local governments provide critical services that make them a critical infrastructure in themselves. They also play an important role as catalyst for public-private partnerships at the community level, particularly for emergency response planning and crisis management. The issue of securing the underlying information networks that support their critical services was a relatively new issue before September 11. State and local governments tend to be well organized as a sector, with multiple common interest groups.

Similar to its program for industry, the CIAO has laid out a plan to implement outreach partnerships with respected and credible channels within state and local government. CIAO has also met with the National Governors Association and the National Association of State Chief Information Officers to encourage input into the National Strategy for Cyberspace Security.

The front lines for the new types of threats facing our country, both physical and cyber, clearly are in our communities and in our individual institutions. Smaller communities and stakeholders have far fewer resources to collect information and analyze appropriate actions to take. Consequently, in February of this year, the CIAO began a series of four state conferences on Critical Infrastructures: Working Together in a New World, designed to collect lessons learned and applied from the events of September 11 from New York, Arlington, and communities across the United States. The intent of this conference series is to deliver a compendium of community best practices at the end of the first quarter of 2003. The first conference was held in Texas and the second in New Jersey. The last two will be held in the latter part of 2002 and the first quarter of 2003.

B. Support for Federal Government Infrastructure Activities

Homeland Security Information Integration Program: The Administration is proposing in the President's Fiscal Year 2003 budget request to establish an Information Integration Program Office (IIPO) within the CIAO to improve the coordination of information sharing essential to combating terrorism nationwide. The most important function of this office will be to design and help implement an interagency information architecture that will support efforts to find, track, and respond to terrorist threats within the United States and around the world, in a way that improves both the time of response and the quality of decisions. Together with the lead federal agencies, and guided strategically by the Office of Homeland Security, the IIPO will: (a) create an essential information inventory; (b) determine horizontal and vertical sharing requirements;

(c) define a target architecture for information sharing; and (d) determine the personnel, software, hardware, and technical resources needed to implement the architecture. The foundation projects will produce roadmaps (migration strategies) that will be used by the agencies to move to the desired state.

Federal Asset Dependency Analysis – Project Matrix: The CIAO also is responsible for assisting civilian Federal departments and agencies in analyzing their dependencies on critical infrastructures to assure that the Federal government continues to be able to deliver services essential to the nation's security, economy, or the health and safety of its citizens, notwithstanding deliberate attempts by a variety of threats to disrupt such services through cyber or physical attacks.

To carry out this mission, the CIAO developed "Project Matrix," a program designed to identify and characterize accurately the assets and associated infrastructure dependencies and interdependencies that the U.S. Government requires to fulfill its most critical responsibilities to the nation. These are deemed "critical" because their incapacitation could jeopardize the nation's security, seriously disrupt the functioning of the national economy, or adversely affect the health or safety of large segments of the American public. Project Matrix involves a three-step process in which each civilian Federal department and agency identifies (i) its critical assets; (ii) other Federal government assets, systems, and networks on which those critical assets depend to operate; and (iii) all associated dependencies on privately owned and operated critical infrastructures.

Early experience with the CIAO's Project Matrix process has demonstrated such significant utility that the Office of Management and Budget has recently issued a directive requiring all Federal civilian agencies under its authority to fund and perform the analysis.

C. Integrated National Strategy for Critical Infrastructure Assurance

Finally, the CIAO also plays a major role with respect to the development and drafting of the two national strategies relating to critical infrastructure protection – the National Strategy for Cyber Space Security and the National Strategy for Homeland Security. Specifically, the CIAO coordinates and facilitates input from private industry, as well as state and local government, to the national strategies. The Office of Homeland Security has enlisted the CIAO to provide coordination and support for its efforts to compile information and private sector input to its strategy to protect the physical facilities of critical infrastructure systems. The CIAO, working with its private sector partners, also has been instrumental in coordinating input from the private sector to the cyber space security strategy.

Conclusion

The American economy is the most successful in the world. However, in the information age, the same technological capabilities that have enabled us to succeed can now also be turned against us. Powerful computing systems can be hijacked and used to launch attacks that can disrupt operations of critical services that support public safety and daily economic processes.

As the President and Governor Ridge have noted, today no Federal Agency has homeland security as its primary mission. Responsibilities for homeland security are dispersed throughout

the Federal Government. The President's plan would combine key operating units that support homeland security so that the operations and activities of these units could be more closely directed and coordinated. This will serve to increase the efficiency and effectiveness of the Federal Government's critical infrastructure assurance and cyber security efforts.

The CIAO looks forward to continuing its role in advancing critical infrastructure protection policy in the new Department of Homeland Security. Thank you for the opportunity to appear before you today. I welcome any questions that you may have.

Mr. HORN. Well, thank you very much. Let us now move to Stanley Jarocki, chairman of the Financial Services Information and Analysis Center and vice president of Morgan Stanley IT Security.

STATEMENT OF STANLEY R. JAROCKI, CHAIRMAN, FINANCIAL SERVICES INFORMATION AND ANALYSIS CENTER, AND VICE PRESIDENT, MORGAN STANLEY IT SECURITY

Mr. JAROCKI. Mr. Chairman and members of committee, thank you for this opportunity to testify about the importance of information sharing and the protection of this Nation's critical infrastructure. It is an honor to appear before you as we discuss these matters in our efforts to further the protection of our great Nation. My name is Stash Jarocki and I come before you to speak from a perspective formed by three decades of experience in the information security field and also as founder and present chairman of the Financial Services Information Sharing and Analysis Center. The FS-ISAC is the first of the private sector's Information Sharing and Analysis Center created in response to PD–63. This directive called for the establishment of these centers to assist sector efforts in the protection of critical infrastructure components from the cyber and the physical world.

I have come before you today to speak about terrorism, both the cyber and the physical, and one of the successful approaches for mitigating its risks. I will also discuss the obstacles to this approach and the steps necessary to address impediments that will slow our successful battle against infrastructure threats. I would like to begin by asking us all to consider the nature of cyber terrorism. It is not merely a creation of an attention hungry, sensationalized media, or the result of panicked public outcry. Cyber terrorism is as much of a threat to us as the painfully realized danger of its counterpart, physical based terrorism. Its implications are far reaching, as the potential for cyber-based terrorism is directly proportional to the pervasiveness of possible targets.

Due to the utter saturation and dependence on a technology-based infrastructure, the realities of the dangers of cyber terrorism must be acknowledged. We may begin with the sad fact that our information technology systems are already under attack and we have every reason to believe that these threats will worsen as we go forward. Also, it lives and depends on a physical environment that has been harshly attacked and could be attacked again and again, not only by man but by the natural forces that exist.

We must act, and we must act quickly. Furthermore, we are not powerless. Just as it is our physical and cyber infrastructure systems that are subject to these attacks, it is our ability to share and exchange information that can provide us with a strong foundation for defense.

Today, there are some 57 of the largest financial institutions, banks, brokerages, insurances and SROs, which represent more than 50 percent of all the credit assets who are members of the FS-ISAC.

Our mission is straightforward: Through information sharing and analysis, provide its members with early notification of computer vulnerabilities and access to subject matter expertise and other relevant information such as trending analysis for all levels

of management and first responders. In fact, we are embarking on a major effort to be the information dissemination pipeline for the entire financial sector, comprised of clients that use our systems to the family run bank to the largest multinational financial institutions. We are joined in this endeavor by other organizations with similar missions. These include the National Infrastructure Protection Center, NIPC; U.S. Secret Service, especially their New York Electronic Crimes Task Force; the Department of Defense's Joint Task Force for Computer Network Operations and others trying to create an effective and trusted network of government and private sector entities sharing information to collectively benefit critical infrastructure protection.

Unfortunately, I am here today to tell you that we cannot succeed in this mission without your help. Legitimate concern has arisen among members of the private sector that has directly affected information sharing, the result of a legislative environment that is not conducive to our best infrastructure protection efforts. We believe there are three actions that must be taken in order to remove legislative obstacles that block effective, robust sharing:

One, provide a narrowly written exemption to FOIA for critical infrastructure information voluntarily shared from private companies or private sharing groups to the Federal Government.

Two, provide an exemption or guidance under the antitrust laws on both a Federal and State level to critical infrastructure information voluntarily shared in good faith within the private sector, especially with a formal structure like the ISACs.

And, finally, provide safe harbor legislation similar to that provided for Y2K to protect the disclosure of infrastructure information within the private sector as long as such disclosure is made in good faith.

We have heard a lot. The risk is too great. Better to keep your mouth shut. Better safe than sorry. These statements represent the danger we face today because that is the kind of advice by general counsels throughout the Nation. We faced this danger before, preparing for the Y2K turnover. In the Y2K effort we avoided it through thoughtful and balanced legislation. We must avoid that danger again. While legislation alone will not solve all the challenges in information sharing, it will go a long way in providing the protection industry needs as well as demonstrating the government's commitment and desire to be an active member of the information sharing process.

As a founder and supporter of the ISAC concept and practitioner in the information security world, I can state that information security is essential.

Finally, effectively robust information sharing becomes the foundation for mapping trends and developing actuarial tables needed to create a factual basis for risk management and a stabilized, insurable environment, thereby reducing the risk that industry sectors must manage on a daily basis.

Mr. Chairman, I would like to thank the committee for permitting me to testify on this important subject. I will be pleased to answer any questions you may have at this time. Thank you.

[The prepared statement of Mr. Jarocki follows:]

STATEMENT OF

STANLEY R. JAROCKI

CHAIRMAN, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER, LLC
and
VICE PRESIDENT, MORGAN STANLEY IT SECURITY

BEFORE THE SUBCOMMITTEE ON GOVERNMENTAL EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS
UNITED STATES CONGRESS

JULY 24, 2002

Mr. Chairman and Members of the Committee, thank you for this opportunity to testify about the importance of information sharing in the protection of this nation's critical infrastructure. It is an honor to appear before you as we discuss these matters in our efforts to further the protection of our great nation.

My name is Stanley R. Jarocki (Stash) and I come before you to speak from a perspective informed by three decades of experience in the information security field and also as a founder and present Chairman of the Financial Services Information Sharing and Analysis Center, LLC - FS/ISAC. The FS-ISAC is the first of the private sector's Information Sharing and Analysis Centers, created in response to May 1998's Presidential Directive 63. This Directive called for the establishment of these centers to assist sector efforts in the protection of critical infrastructure components from cyber and physical threats.

I've come before you today to speak about Terrorism – both Cyber & physical - and one of the successful approaches for mitigating its risk. I will also discuss the obstacles to this approach, and the steps necessary to address impediments that will slow our successful battle against infrastructure threats.

I would like to begin by asking us all to consider the nature of Cyber Terrorism. It is not merely the creation of an attention hungry, sensationalized media, or the result of panicked public outcry. Cyber Terrorism is as much of a threat to us as the painfully realized danger of its counterpart - physical-based terrorism. Its implications are far reaching, as the potential for cyber-based terrorism is directly proportional to the pervasiveness of possible targets.

Governor Tom Ridge recently stated:

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

Due to the utter saturation and dependence on a technology-based infrastructure, the realities of the danger of Cyber Terroism must be acknowledged. We may begin with the sad fact that our information technology systems are already under attack and we have every reason to believe that these threats will worsen as we go forward. Also, it lives and depends on a physical environment that has been harshly attacked and could be attacked again and again not only by man but by the natural forces. There are

many indications of the increased danger to cyber based information assets, as evidenced by the following small sampling of current events:

- According to a recent report of the National Research Council, U.S. companies spent $12.3 billion to clean up damages from computer viruses in 2001, with damages in 2002 expected to exceed those of 2001.
- The 2002 CSI/FBI survey found that 90% of companies surveyed admitted to a successful computer breach in the preceding year, resulting in hundreds of millions of dollars in quantifiable losses.
- Mass cyber-events such as "I Love You" virus, the Melissa Virus and the recent Code Red and NIMDA viruses are reported to have caused hundreds of millions of dollars in damages.
- Finally, the CERT Coordination Center at Carnegie Mellon announced that in 2001 they received over 50,000 incident reports, a two hundred percent growth in reports from 2001 and a four hundred percent growth from year 2000.

Today, some say it would be easier for a terrorist to attack a dam by hacking into its command and control computer network than it would be to obtain and deliver the tons of explosives needed to blow it up. Even more frightening, such destruction can be launched remotely, either from the safety of the terrorist's living room, or their hideout cave.

We must act and we must act quickly. Fortunately, we are not powerless. Just as it is our physical and cyber infrastructure systems that are the subject of these attacks, it is our ability to share and exchange information that can provide us with a strong foundation for defense.

I have had the honor of participating in a successful information sharing organization with the building of the FS-ISAC and it is my pleasure to speak with you about the benefits of such an Experience. In October 1997, the *Report of the President's Commission on Critical Infrastructure Protection* identified the banking and finance sector as critical to the nation's well being. This finding incorporated in PDD-63 sparked the banking, brokerage, and insurance industry to action. With the support of the US Department of Treasury, Secretary Lawrence Summers launched the Financial Services Information Sharing and Analysis Center on October 1, 1999 with an initial roll of 11 members. Today there are some 57 of the largest financial institutions – banks, brokerages, insurance and SROs, which represent more than 50% of all credit assets, who are members of the FS/ISAC.

The mission of the FS/ISAC is straightforward: Through information sharing and analysis provide its members with early notification of computer vulnerabilities and attacks and access to subject matter expertise and other relevant information such as trending analysis for all levels of management and first responders. In fact, we are embarking on a major effort to be the information dissemination pipeline for the entire financial sector comprised of the clients that use our systems to family run banks to the largest multi-national financial institutions.

We are joined in this endeavor by other organizations with similar missions. These include the National Infrastructure Protection Center (NIPC); US Secret Service, especially the NY Electronic Crimes Task Force; the Department of Defense's Joint Task Force for Computer Network Operations and others trying to create an effective and trusted "network" of government and private sector entities sharing information to collectively benefit critical infrastructure protection.

Unfortunately, I am here today to tell you that we cannot succeed in this mission without your help. Legitimate concern has arisen among members of the private sector that has directly affected information sharing, the result of a legislative environment that is not conducive to our best infrastructure protection efforts. Today existing laws and regulations pose severe obstacles preventing the voluntary disclosure of information – regarding threats to and vulnerabilities of critical facilities, networks and supporting systems within the private sector, as well as exchanging between the private sector and the public sector. Fear of violating anti-trust laws, or of exposing sensitive corporate information through FOIA access rights has severely hindered information sharing efforts, a weakness that must be addressed if our nation is going to deal with the proliferation of information based threats. The private sector safeguards much of the critical infrastructure and is in a large part responsible for the economic success of the United States. At our disposal we have an incredible abundance of resources and information, but we must be given the freedom to leverage it effectively. We believe that there are three actions that must be taken in order to remove legislative obstacles that block effective, robust information sharing:

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

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

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

These actions would go far in alleviating the hindrances to information sharing for the private sector. Our concerns are predicated on some of the very same forces that allow our economic and governmental system to operate as effectively as it currently does. Along with the potential violation of either federal or state anti-trust laws, the sharing of information may lead to liability lawsuits against the company or its officers and directors.

The chilling effect of potential liability lawsuits on voluntary speech cannot be underestimated. The fear of litigation has always played an important role in fostering proper conduct. However, when applied inappropriately, it can have the opposite impact – that of chilling desirable conduct.

Such is the situation here. Why disclose the potential inadequacies of your vendor's security technology when your general counsel tells you that the disclosure could lead to a defamation suit? Why recommend the use of specific technological safeguards when such disclosures could lead to lawsuits alleging tortuous interference with the contractual rights of others who use competing technology? Why freely disclose the results of millions of dollars in research and analysis of "best practices" when such disclosure could lead to shareholder lawsuits alleging misconduct in disclosing company "trade secrets" or other breaches of the fiduciary duties.

"The risk is too great." "Better to keep your mouth shut." "Better safe than sorry." These statements represent the danger that we face today because that's the kind of advice given by general counsels throughout the nation. We faced this danger before, preparing for the Y2k turnover. In the Y2k effort, we avoided it through thoughtful and balanced legislation. We must avoid the danger again. While legislation alone will not solve all challenges in information sharing, it will go a long way in providing the protections industry needs as well as demonstrating the Government's commitment and desire to be an active member of the information sharing process.

As a founder / supporter of the ISAC concept and a practitioner in the information security and audit world, I can state that information sharing is essential. It can and does raise the awareness of the community to the vulnerabilities and exposures that they face and permits responsible exchange of information amongst the legitimate stakeholders and defenders to work collectively and individually towards resolutions and solutions to these problems. This enhances and migrates the culture of the critical infrastructure sectors to preventive postures and strengthens the environment that is under constant attack. Furthermore, timely, protected information sharing enables the critical infrastructure sectors to work with the vendor community and their technologists in a trusted environment to develop fixes and deploy them in a timely manner prior to public disclosure. This then can be a significant portion of the foundation for responsible disclosure and the exercise of "sound business" practices. Finally, effective and robust information sharing becomes the foundation for mapping trends and developing actuarial tables needed to create a factual basis for risk management and a stabilized insurable environment thereby reducing the risk that the industry sectors must manage on a daily basis.

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

Mr. HORN. Thank you, Mr. Jarocki. The last presenter is Louis G. Leffler, the Manager-Projects of North American Electric Reliability Council. I am very fascinated by your companion councils around the country, so you might just like to tell us a little bit about it before you start in on the substance of all this.

STATEMENT OF LOUIS G. LEFFLER, MANAGER-PROJECTS OF NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Mr. LEFFLER. Thank you, Mr. Chairman, and thank you for this opportunity to present some of the work of the electricity sector directed at securing our critical infrastructure from cyber and/or physical attack with specific emphasis on the Electricity Sector, Information Sharing Analysis Center.

Regarding NERC, the North American Electric Reliability Council was formed in the aftermath of the 1965 power system failure in the Northeast; it was formed actually in 1968. There are currently 10 regional councils which includes all of the United States, virtually all of Canada and a very small part of Mexico.

One of the points that is made in the testimony, and I will make it here, is that electricity is unique. All the critical infrastructures have their own unique characteristics. One of the uniquenesses of ours is that electricity is an on-demand product. It is made the moment it is required. And one other point that is extremely important in what we are trying to do here, is that we are all connected. We are all interconnected. Virtually every single power producer, power transmission system and distribution grid one way or another is connected with every one. So what happens to one may very well impact what happens to another.

Therefore, it is imperative and absolutely essential that we coordinate and have the policies in place on how we operate the system so this system is operated reliably to avoid another cascading power system failure, be it due to any myriad of possible things like bad weather, equipment malfunction or a terrorist attack. That is a little bit of a sum-up as to what NERC is.

Mr. HORN. Thank you. We will now go into the question period.

Mr. LEFFLER. I am not done.

Where interdependencies were mentioned before, I mention them now within our sector, and of course they exist between our sector and the others. We did an exercise years ago on Governor's Island in New York, and it was interesting. It was 10 years ago or more, brought together all these same critical infrastructures and we sat around a table and the challenge was, here it is Sunday morning, snowstorm coming, terrorists have come in and shut down a major power system and you are all here. President is at Camp David and he is coming back to the White House at 3 o'clock in the afternoon, what are you going to tell him? So we sat around and looked at ourselves and started to come up with solutions. Some interdependency problems, some of the things that one of the other presenters spoke about regarding this intricate linkage of the interdependencies and so on.

Our sector is well equipped for a panoply of events. I already said that. We established—and then we really established right after the PDD–63 was promulgated by the last administration—a group to start dealing with this, and we began meeting with our

sector liaison, which is the Department of Energy, and immediately following that we found out about an organization called the National Infrastructure Protection Center and began working with Ron Dick and his people over there. We established excellent relationships.

In order to do this for the electricity sector so it was done once and done well for the entire sector, we created a thing called the Critical Infrastructure Advisory Group and it represents the subject matter experts in physical security, cyber security and operations from all the industry segments. And it is working pretty well; it reports directly to the NERC board of trustees.

We also worked with—I mentioned the Department of Energy and the NIPC, the Department of Defense, the Critical Infrastructure Assurance Office, the Nuclear Regulatory Commission and the Federal Energy Regulatory Commission, the FERC. The testimony goes into a lot of what we have done. I am not going to repeat that here.

We do have a set of security guidelines, both physical and cyber. We have one on security of data that we think is extremely important and we are working with the FERC on including appropriate security measures in the standard market design for electricity.

Our ISAC was established about the same time that we initiated the IAW—Indications, analysis, waring program—with the NIPC. That was in October 2000. The mission is to receive information for analysis, provide interpretive analytical support to the NIPC and other government agencies, and disseminate threat warnings together with interpretation to guide the sector. The staff with NERC personnel is available to any electricity sector entity at no charge.

What can the government do to encourage information sharing? We already talked quite a bit around this table about the need for some considerations to FOIA. I am not an expert in this area, but it has been said very well that we want to voluntarily share this information. We need to voluntarily share this information, and we need some additional limited protections in that area.

We request faster granting of U.S. clearances. We have a number of clearances. The ISAC people have them. A number of people in the industry do, and we need them to enhance our capabilities for analysis and understanding.

The very essence of ISAC operations requires communications. We must increase the availability of reliable and secure telecommunications for use among sector participants, the government and the ISAC. The electric industry operates in a constant state of preparedness planning, training and operating synchronous grids, requires preparedness for natural disaster energy emergencies and the attacks of sabotage or terrorism.

We greatly appreciate our working relationships with the government agencies and look forward to answering any questions you may have for us. Thank you.

[The prepared statement of Mr. Leffler follows:]

Testimony to

The United States House of Representatives

Committee on Government Reform

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Discussing

Activities Undertaken by the Electricity Sector to Address Physical and Cyber Security with Emphasis on the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)

Prepared by
Louis G. Leffler, Manager-Projects
North American Electric Reliability Council

July 24, 2002

Activities Undertaken by the Electricity Sector to Address Physical and Cyber Security with Emphasis on the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)

Thank you for the opportunity to present to the Subcommittee's oversight hearing on Cyber Terrorism and Critical Infrastructure Protection some of the concepts being established by the Electricity Sector to enhance the security of our Nation's critical infrastructures.

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

In addition to its job of "keeping the lights on," NERC serves as the electric industry's contact and coordinator in the United States and Canada for bulk electric system security matters and operates the Electricity Sector's Information Sharing and Analysis Center (ES-ISAC).

In my role, I have the responsibility to facilitate the work of NERC's Critical Infrastructure Protection Advisory Group; I am a member of the ES-ISAC team, and Sector Coordinator.

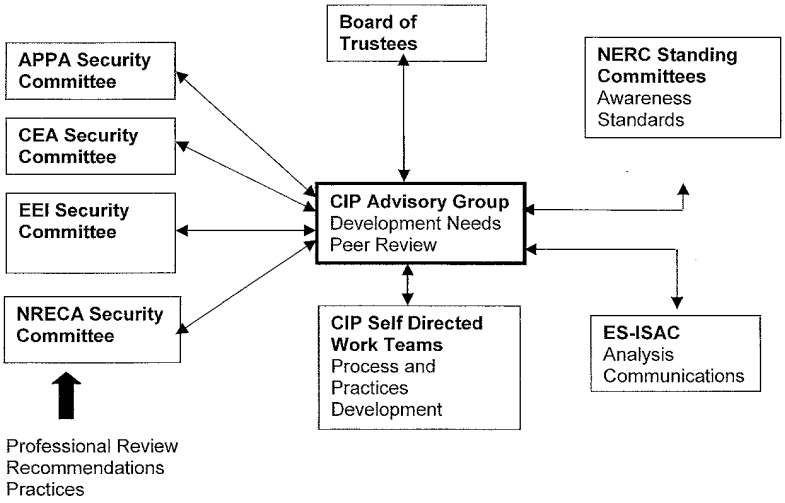
We have been requested to provide a description of the security actions taken by the Electricity Sector with primary emphasis in this testimony focused on the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

Before delving into ISAC and related matters, let me state that NERC supports the National Strategy for Homeland Security presented by the President last week. Some legislative recommendations are discussed herein.

Organization

Following issuance of the President's Commission on Critical Infrastructure Protection in 1997 and the President's Decision Directive 63 in 1998, the Secretary of the U.S. Department of Energy requested NERC to accept the role as Electricity Sector Coordinator (for Critical Infrastructure Protection). NERC President and CEO, Michehl Gent, with approval of our Board of Trustees, accepted this assignment as a logical extension of NERC's mission. NERC established a study and action group — which is now the Electricity Sector Critical Infrastructure Protection Advisory Group (CIPAG) with a direct reporting relationship to the NERC Board. Essential to progress in our efforts to enhance security of the Electricity Sector is the cooperation of all segments within the Sector. The CIPAG brings together the generation and transmission providers, public and investor-owned utilities, power marketers, regional transmission organizations and independent system operators, electric power associations, and government agencies. Both Canadian and United States entities participate.

The CIPAG is organized as depicted below.



APPA	American Public Power Association
CEA	Canadian Electricity Association
EEI	Edison Electric Institute
NRECA	National Rural Electric Cooperative Association

Indications, Analysis, and Warning Program

After the CIPAG established its relationship with our Sector Liaison, the U.S. Department of Energy (DOE), the advisory group and representatives of the DOE met with the National Infrastructure Protection Center (NIPC). From this has emerged a close security working relationship that resulted in the development of the Electricity Sector – NIPC Indications, Analysis, and Warning Program (IAW Program).

(From the IAW Program):

> This SOP (Standard Operating Procedure) establishes voluntary procedures for implementing the information reporting, analysis and warning provisions of the National Infrastructure Protection Center's (NIPC) national level Indications, Analysis & Warning (IAW) program for electric power. This program has been established to enable the NIPC to provide timely, accurate, and actionable warning for both operational and cyber threats or attacks on the national electric power infrastructure.

The IAW Program provides several reporting mechanisms to enable reliable and secure communications between Electricity Sector entities and the NIPC. The IAW Program SOP contains event criteria and thresholds with report timing for nine physical/operational and six cyber/social engineering "event types." Those events to be reported include those occurrences to an Electricity Sector entity that are either of known malicious intent or are of unknown origin. Events include such things as the loss of a key element of an electric power system or telecommunications critical to system operations, announced threats, intelligence gathering (surveillance), computer system intrusion (each event type contains specificity as to level of actual or potential impact on operations of the reporting electric entity). Note

that electric "entities" include generation, transmission, distribution, overall system reliability coordination, power marketing.

The power of the IAW Program lies in the fusion of incident information from many sources (government and private sectors) in one place for continuous analysis and prompt dissemination of threat and possible vulnerability information back to the sectors.

The IAW Program was approved for voluntary use by the Electricity Sector in July 2000. Over the next several months, NERC and NIPC conducted three workshops designed to raise the Sector's awareness to the security issues and to introduce the IAW Program. The program is in use currently.

Electricity Sector — Information Sharing and Analysis Center (ES-ISAC)®

The ES-ISAC was formed to:

- Obtain security information related to possible threats or suspicious activity, or actual malicious or terrorist acts against the Electricity Sector and to assure that this information is provided to the NIPC for analysis.
- Assist the NIPC in its analysis of the actual or potential impact of threat to or vulnerabilities of the Electricity Sector. Subject matter expertise may be provided directly by ISAC personnel or through contact with Sector people arranged via the ISAC.
- Immediately disseminate threat and vulnerability warnings on a Sector, geographic, facility type, specific facility basis as appropriate.
- Provide ongoing Sector awareness to the ever-changing security landscape.

With Board approval, NERC announced the ES-ISAC in October 2000. This function has grown in capability and support since then. It is staffed by NERC personnel who consult with particular subject

matter experts throughout the Sector. The CIPAG provides functional oversight to the ES-ISAC with regular review at each meeting.

The ES-ISAC Mission

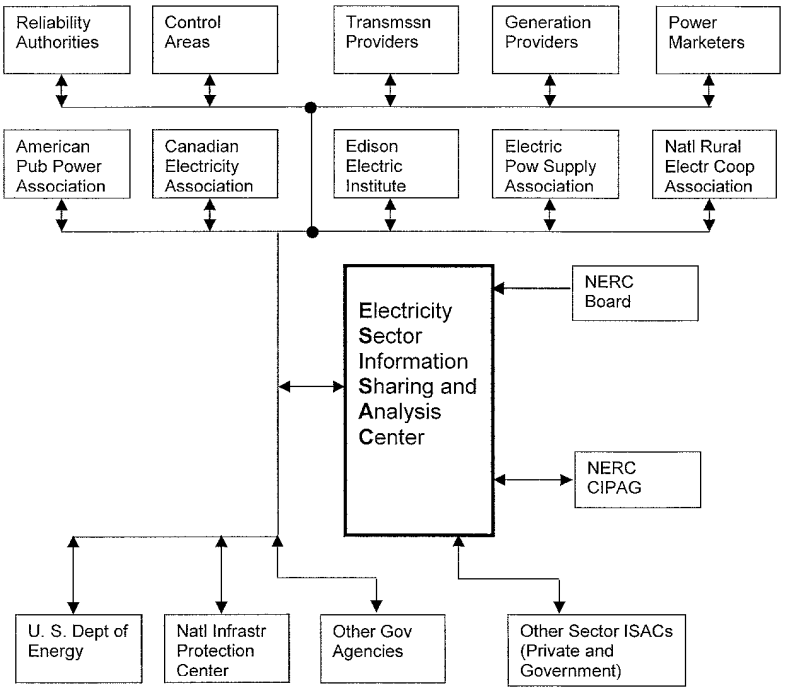
- Receive Electricity Sector information for analysis by government agencies and the ISAC.
- Provide analytical support to the NIPC and other government agencies in the interpretation of information relevant to the Electricity Sector.
- Promptly disseminate threat indications, analyses, warnings together with interpretations to assist the Electricity Sector in taking protective actions.

ES-ISAC Objectives

- As Electricity Sector Coordinator work closely with the U.S. Department of Energy (Sector Liaison) and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness.
- Assist the National Infrastructure Protection Center (NIPC) in incident analyses.
- Receive incident data from all ES entities.
- Disseminate threat and vulnerability assessments to ES entities.
- Liaison with other government and private ISACs.
- Analyze Sector interdependencies.
- Participate in infrastructure exercises.

The ES-ISAC Organization is depicted below.

ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS CENTER



(All data and information streams depicted above are voluntary.)

A Few ES-ISAC Particulars

- There are currently seven NERC employees detailed to the ES-ISAC. The actual amount of time spent on ES-ISAC duties by each individual varies.

- The ES-ISAC has established multiple communications including telephone, secure telephone (STU-3), fax, satellite phone, pagers, secure messaging system, e-mail listservers, Internet site. The ES-ISAC is not currently staffed 24x7; staff is on 24x7 call.

- The ES-ISAC and the CIPAG coordinate with many organizations, including:

  - American Gas Association
  - American Petroleum Institute
  - American Public Power Association
  - Canadian Electricity Association
  - Critical Infrastructure Assurance Office
  - Department of Defense
  - Department of Energy and several National Laboratories
  - Department of the Interior
  - Edison Electric Institute
  - Electric Power Supply Association
  - Electricity Consumers Council
  - Federal Energy Regulatory Commission
  - National Infrastructure Protection Center
  - National Rural Electric Cooperative Association
  - Nuclear Energy Institute
  - Nuclear Regulatory Commission
  - Oil and Gas Sector
  - Partnership for Critical Infrastructure Security
  - Rural Utility Services

- The ES-ISAC is funded as part of the NERC budget which is approved by the independent Board of Trustees. There are no fees to those participating Electricity Sector entities.

Other Security-Related Activities

Following are other activities undertaken by NERC:

- Published an Approach to Action for the Electricity Sector

- Published Security Cases for Action for the Electricity Sector

- Developed a set of Security Guidelines:
  - Executive Summary
  - Communications
  - Emergency Plans
  - Employee Background Checks
  - Physical Security
  - Threat Response
  - Vulnerability Assessments
  - Continuity of Business Practices
  - Cyber Security: Access Controls
  - Cyber Security: Firewalls
  - Cyber Security: Intrusion Detection Systems
  - Cyber Security: Risk Management
  - Protecting Potentially Sensitive Information
- Developed Threat Alert Levels
  - Physical
  - Cyber

The above documents are available via the NERC and ES-ISAC Internet sites:

- <http://www.nerc.com>
- <http://www.esisac.com> (under development)

What Government Can Do to Encourage Information Sharing

The more information that is shared among and between government agencies and ISACs, the better will be each of the ISAC's ability to respond to the threats we may face and vulnerabilities we may have. But this raises concerns about the consequences of unauthorized public disclosure of highly sensitive information. Specific areas for policy consideration follow.

- Congress is in the best position to mitigate the security risks inherent in information-sharing activities, whether voluntary or required. As to voluntary information-sharing, Senators Robert Bennett (R-UT) and Jon Kyl (R-AZ) have introduced legislation, S. 1456, that would promote voluntary information sharing about sensitive security issues among critical infrastructure entities, and between those entities and the government by providing limited, specific clarifications of the

Freedom of Information Act (FOIA) and of federal antitrust laws for certain critical infrastructure protection information sharing efforts by the private sector.

- We recommend revisions to the Freedom of Information Act to permit more sharing of certain information with the government that may be critical to analysis, but not of general need by the public. We understand that the Committee on Government Reform has recommended including FOIA relief as part of the Homeland Security Bill, and we thank the Committee.

- We have concern for the ease of access to sensitive and perhaps vulnerability revealing electricity system information. We fully recognize the need to provide electric power system information to those operating, overseeing, regulating, or otherwise managing the power system, and we recommend more definition of the relevant access.

- We recommend revisions to antitrust laws to permit more freedom to share information among Electricity Sector entities that may be critical to analysis. Because the electric industry is very tightly interconnected on a physical basis, cooperation is requisite. Now a new area of cooperation has arisen — security.

- We request more rapid response to the requests for granting U.S. government clearances to key Electricity Sector personnel to permit the capability to more fully analyze and understand the threats to the Electricity Sector and to interdependent infrastructures.

- The very essence of ISAC operations and resultant value add to any sector requires communications. We must increase the availability of reliable and secure telecommunications for use among Sector participants, the government, and the ES-ISAC.

Conclusions

In conclusion, I would like to make these points:

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

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

- NERC serves as the electric industry's contact and coordinator in the United States and Canada for bulk electric system security matters and provides the ES-ISAC.

- Coordination and cooperation among all Electricity Sector participants and with government agencies will continue to be the key to security.

We greatly appreciate our close relationship with the Department of Energy (our Sector Liaison), the National Infrastructure Protection Center (our partner in the IAW Program), the Critical Infrastructure Assurance Office, and the Federal Energy Regulatory Commission.

Thank you very much for this opportunity to present the work undertaken by the Electricity Sector with the support of several government agencies to help secure the Electricity Infrastructure of the United States and Canada.

Mr. HORN. Thank you. We will now have the question period, and it will alternate between Ms. Schakowsky, the ranking member, and myself, and we will do 5 minutes each so everybody gets a chance here. So Ms. Schakowsky, 5 minutes.

Ms. SCHAKOWSKY. Well, I am hearing the drum beat of FOIA and while there are many other things to focus on, I want to focus on that because I am very disturbed about what I am hearing. I was particularly concerned and I quoted in my opening statement, Mr. Dick, a remark of yours that talks—that says, "if the private sector doesn't think the law is clear, then by definition it isn't clear."

It seems like that's the theme of the day—have talked about not a conducive atmosphere for the private sector to share, and therefore we should change FOIA. I would just want to suggest there is another option, and that is to say this information isn't voluntary, that we require it; that this is a time of a war on terrorism, and that we are calling on individuals and businesses to be patriotic and to provide information. I just—I'm not suggesting I am going to introduce anything of the sort, but I wanted to just say that this is a critical time, we all agree, that's why we are here today to discuss it. That we could, in fact, just say that because this is so critical to our national security, our homeland security, we could simply require this rather than, in my view, pander to the desires of businesses to keep information secret, an item that's been on that agenda for many years, not just now.

And when I see public officials saying that individuals—because that's what we're saying—individual citizens should be deprived of information that is—now, we have a Freedom of Information Act, and I want to talk to you about that, that has nine exemptions to protect information from the public when necessary. And such exemption b(4) deals with trade secrets, confidential business information, protecting—and I know, Mr. Dick, you don't think that's sufficient. And, so in addition, we have Executive Order 12600 that says if information is to be released and a business objects, there is a whole procedure to stop that information from being released.

And it astounds me that at a moment in history when transparency in business is on the headlines every day, the need for us to know what is going on in our private sector, which has deprived many of our citizens of their ability to retire and employees of their future retirement plans, sends the stock market diving because of this lack of transparency, cooking the books, that now we want to offer, in my view—and I want your opinion on this—not a narrowly constructed exemption to FOIA, but a loophole big enough to drive any corporation and its secrets through, in my view. One that says that if they simply declare it to be—to need to be secret, that not only in an amendment that would—I think may be part of the bill—is that 12, Department exemption now, the Davis amendment? Homeland Security.

So now if a company wants to protect information from public view, they could dump it in the Department of Homeland Security and say we don't want anyone to have access to it because it's critical information, and it could be something that communities need to know, about pollution of a chemical plant or etc.

I think we ought to be concerned about these abridgements of individual rights to information, and have a little more concern about

that than we seem to be exhibiting today about the lack of interest of private businesses at this time of war to share critical information.

If I seem outraged, it is only because I am. So I would like some response.

Mr. TRITAK. I would like to take this, if I may just comment on a couple things. One is the administration's position has been very clear. One—this is supposed to be a narrowly crafted exemption.

Ms. SCHAKOWSKY. And do you think this one is?

Mr. TRITAK. Well, let me—what I would like to say is what the administration's position has been. Right now, you are in the give-and-take process of creating law. If things aren't as clear as they need to be, this is the time to work on them. I can tell you what the President has made clear about what the intentions are: It is to be narrowly crafted. It is not to be a permit or a process for data dumping—if I may finish, please.

Also, we are talking about voluntary information, as we said before. Now, you just presented an alternative to that. But the point is, right now, today, there is information of the kind that right now is not mandatorily required that could help safeguard the homeland through a voluntary sharing regime? I think the answer is yes. But no one is talking about creating a safe haven for negligence or a safe haven for criminal activity.

Now, what I said before, that we are talking about a culture collaboration, I don't want that to be viewed as a synonym for a culture of coddling. What we are talking about here is we have a shared responsibility, and we have got to manage it properly. If the existing provisions that have been put forward suggest otherwise than what the President has made clear and has been his position before, then it seems to me this is the give-and-take process——

Ms. SCHAKOWSKY. What does the administration think about it? Is it narrowly focused enough for the administration, the current language that we are going to be considering tomorrow or Friday? This is not imaginary language. There is language.

Mr. TRITAK. No. Look, I am aware of the concerns that have been expressed, and they have been expressed quite a bit. I am also aware that there has been a fairly active dialog to address those concerns and to bring this into—my sense is that the new provision is going to look a lot different from the one that exists today. So that's why——

Ms. SCHAKOWSKY. That's not my understanding.

Mr. TRITAK. Well——

Ms. SCHAKOWSKY. We're going to try, certainly.

Mr. TRITAK. Well, but I think this is in fact an active dialog that's happening between the administration and the Congress as we speak.

Ms. SCHAKOWSKY. No, I think that's really a copout, because there is language, as was proposed by the administration, that is currently in the bill. I will be offering an amendment, I hope it will get bipartisan support, that will change that language. But it's not theoretical or—I mean, it is written right now in a piece of legislation. And I want to know if that is the language that you think is narrowly crafted enough, and that's the administration's language.

Mr. TRITAK. I think the position the administration put forward is the one that it believes would advance the issues I have just addressed. I also think that people recognized going in that this was going to be a provision that was going to be worked. So the real question at the end of the day is, the final bill that is going to pass both the House, the Senate, and the administration, is going to reflect a consensus on this matter. And I can only tell you that what the administration has been fairly clear on is that this is not intended to be an open-ended, overly broad information sharing process; it is meant to provide clarity and certainty to the stakeholders of the infrastructure as to what is in and out of bounds in terms of what is protected under FOIA.

Ms. SCHAKOWSKY. So the language in the Armey bill—that's the bill right now—came out of the select committee. That's the bill, that's the language. Is that the—does the administration support that language currently?

Mr. TRITAK. You know, what I have to tell you, I think that there currently is a review about that language as part of the administration's response, and I would rather not say anything about it at this time. But I take the point, and——

Ms. SCHAKOWSKY. OK.

Mr. TRITAK [continuing]. All——

Ms. SCHAKOWSKY. But, no. Let me ask—can I ask another quick question?

Mr. HORN. Certainly.

Ms. SCHAKOWSKY. What efforts have been made to let the private sector that might have this critical information know about how to use the existing FOIA act, about the Executive order, and to create a sense of comfort—which, I guess, is what we need to do. It seems to me that the tools are here. It doesn't surprise me that the private sector might want to go further. But have there been efforts, particularly post-September 11th, when we are trying to get this information, to encourage that information and to make it clear how to use the current tools?

Mr. DICK. I will take that one. Since the inception of the ITC, one of the issues that has continually come up, as I said in my oral statement, is this very issue. We have had a continual dialog with the ISACs, the InfraGard members, which, as I said, total over 5,000, and anyone else that we can get in front of, and try and clarify and explain how the government would be able to protect information under the FOIA exemptions.

The reality is, though, for example, in the Trade Secrets Act, one of the things that I am told—I am not a lawyer—that if there is a request for that, the industry would have to come forward and discuss in court what it had done to protect that information. So therefore, they would have to go into court and prove, I assume beyond some standard, that they had adequately protected it in the first place.

One of the things you have to keep in mind is that the information that we are talking about is owned by the private sector, and FOIA does not apply to the private sector; it only applies to the executive branch.

So we are talking about information that the private sector believes is sensitive and are concerned about it being disclosed, and

they have questions as to whether the government can adequately protect it. And what we are recommending is not some broad loophole, but a measured response in the language that provides them the assurances that will provide better information sharing.

Ms. SCHAKOWSKY. Well, first of all, my understanding is that you are wrong about the protection of that information. If it is voluntarily provided to the Federal Government and then there is a FOIA request, it is not because it is in that category of voluntary information that it is automatically released and not covered by FOIA; it is now covered by FOIA, and all of those nine exemptions and the Executive order apply to that information.

But I think perhaps a more central question is, do any of you know of any instance, even one, where confidential information has been released by the Federal Government in response to a FOIA request over the objection of the business that supplied that information?

Mr. DICK. The answer is we are not—meaning the NIPC and the FBI—aware of that. But on the flip side of that, because of these concerns, I can't tell you that we are getting an extremely high volume of information either. So it hasn't really been tested.

Mr. HORN. We will move from 5 minutes to 10.

And Mr. Tritak, again, when is the Comprehensive National Infrastructure Protection Plan expected to be completed?

Mr. TRITAK. Well, as you know, the overall homeland security strategy was just released last week. And the next step is that there will be two, what I would consider to be baseline strategies, one dealing with the concerns of the cyberspace security, which is being overseen by Dick Clarke, and the other is the challenges to the physical infrastructures—critical infrastructures, which will be coming out sometime in September or October as well.

It is then the intention of the homeland security effort to create one integrated approach, which would follow sometime thereafter. I think the real answer is as soon as possible, but there hasn't been that date set. But given—frankly, given the pace with which things have been moving, I wouldn't expect it to follow much longer from those releases.

Mr. HORN. Will the proposed plan address specific roles, responsibilities, and relationships for all the critical infrastructure protection entities, establish interim objectives, and set milestones for the achievement, and establish performance measures?

Mr. TRITAK. Yes, that is the intention.

Mr. HORN. OK.

Mr. TRITAK. And I will also add, more infrastructure sectors have been added since PDD–63 to take into account the homeland security issues of food protection and the rest. So, yes.

Mr. HORN. What are the incentives for the private sector to share information with the Federal Government?

Mr. TRITAK. They're a target. And there is also I think a recognition that there are certain pieces of information that the government can provide, once it knows more about the challenges that the private sector is facing, that can help them better do their jobs.

Mr. HORN. What can we do to do anything to improve these various incentives?

Mr. TRITAK. I think one of the purposes of the strategy is to actually—by the way, the strategy that will be coming out in September is actually the product of industry and government working together. And I think what will be extremely important is as we find obstacles to homeland security, some of them may very well raise issues, statutory concerns or otherwise, and then we will be coming to people like you to discuss how we go about dealing with them. And so I think it is the constant vigilance of the Congress as these public issues come to the fore, in which government has to play a role in order to get to advance the cause of homeland security that you will provide the most helpful function in that regard.

Mr. HORN. Do you think the private sector in the State and local governments are willing to fund the efforts required to adequately secure our critical infrastructures?

Mr. TRITAK. I think they are. I think the question is always going to be, particularly with State and local governments, how much of this is quintessentially the roles and responsibilities of the State and local government, and how much is the homeland security proposition at the State and local level really a Federal issue as well.

Governor Ridge has made it very clear that at the end of the day, homeland security is won in the hometown, which is exactly what happened in New York. We were much, much better off because of the brilliant work that was done by New Jersey, Arlington, Virginia and the rest, and the contingency plans that they had done. And we would have been in a lot worse shape if they hadn't been thinking through this problem before.

Mr. HORN. How long will the move to the new Department of Homeland Security improve the Critical Infrastructure Assurance Office's ability to fullfil its mission? Will it stay with Commerce, essentially?

Mr. TRITAK. No. The idea is that it will actually be under the Department of Homeland Security. And I think what it will do is allow us to leverage our resources along with the co-location of people like Ron Dick and others, so that we—basically, we could be more focused. We give industry, for example, single points of contact as opposed to multiple points of contact. It will be more efficient and effective, Mr. Chairman.

Mr. HORN. Well, thank you. That's a good response.

Mr. Leffler, do you believe that the private sector is willing to fund the efforts necessary to adequately secure our critical infrastructure?

Mr. LEFFLER. Absolutely. I think that with—with some help. I think that we have to define very clearly and very carefully what securing this infrastructure really means, and we have begun that dialog. Cyber is one perspective. We heard a lot of discussions on the earlier panel about process control systems. It's an issue that we have on our—under our purview right now. We are seriously considering what needs to be done. It's a big issue, and it does need to be addressed, and we are in the process of commencing that process.

The other one on cyber controls or cyber perspective is the cyber business commerce. And this, I mentioned in my testimony, this is—we are working with the FERC in developing a security stand-

ard for the standard marketing design, and we will work with them in establishing that, promulgating what needs to be done by everybody. Basically anybody who is going to be participating in this industry, will need to step up to the bar on that one.

And then, securing everything in the cyber world, we have another project called Public Key Infrastructure, which we have embarked upon received approval from our board to commence, and we are working that one to do it as well.

Now, we get to physical. And we say, OK, how do we secure this system from physical—from any kind of physical attack? It is everywhere, as everyone knows. And that's an extremely difficult thing to do. So part of the answer is in knowing where critical things are, knowing what things are critical, knowing what we need in the way of spares. Perhaps we can get some support there in establishing spares, locating spares, transporting spares when they are needed to be used. Those are some of the things that we may need some assistance in. And then, finally having excellent—I mean excellent—plans for reconstitution in place, as did ConEd in New York City. Their restoration of that city's electricity, gas, and steam infrastructures was just fantastic.

Mr. HORN. Mr. Jarocki, you probably ought to be in on this dialog here. Any thoughts with what Mr. Leffler thought?

Mr. JAROCKI. I think a lot of the things that are already being done are helpful and an expansion. For instance, let me give you some examples. During—obviously, during the September 11th scenario, the FS-ISAC opened up the ISAC to the entire industry, and we created an eBay type environment that says, what is available? Is there space available? Is there product available? And everything else.

We also found that in order to communicate readily with each other, we needed the exact thing that Lou said. Where is the emergency communications? Through John's office we were able to get a lot of guest cards immediately issued to our executives to start that process, because it is key. When all fails—in New York City, I was a participant in the September 11th exercise. Unfortunately, what worked—it was strange. Two-way pagers worked; cell phones and everything else just went out. And I saw the fear in people's eyes. You know, what do we do? It was a war. It was a definite war, and communications breaking down. I mean, we were lucky at Morgan Stanley because of the redundancy in everything else, our communications did not break down internally; but externally, we were there. So I think there is a lot there.

Wearing my old hat from many, many years ago as an intelligence officer at Fort Meade and working with that group, I think one of the things that we could get from the government is we learned a lot about taking large volumes of data, analyzing it, and being able to extract the fine points that are necessary to make an operation valid and give us value information. I think a lot of that, if we can get at those algorithms, get at that process, is what we need in the civilian community, in the ISACs, so we could start processing, and get at—I think the last time we did a catalog of over 108 Federal data bases which had significant information that we could use that might very well help us out in protecting our infrastructure.

Mr. HORN. How would you characterize the quality and quantity of the data being shared from the Information Sharing Analysis Center to the government?

Mr. JAROCKI. I looked at it—it is sort of a marriage; we're dating, and so we are exchanging information. We haven't gotten to the altar yet. But I think it is a positive thing. You know, you are testing the waters.

You are saying, here it is. It's a very good relationship with the organizations I mentioned: NIPC, the New York Electronic Crimes Task Force. To me, it's a very positive relationship. Again, it was built on one important thing—how can we trust each other—as opposed to having guns and badges. It's a trust of people and exchanging information, and I think it's—it is only getting better.

Mr. HORN. What type of information is shared among Information Sharing and Analysis Center members but not with the Federal Government?

Mr. JAROCKI. Right now I will only reflect on the technology side, is we share an awful lot of information on what's technology and, specifically, what might be within our own realm of the financial sector, this piece of software or whatever we have. Is that shared with other sectors? No, because it's not germane to them. But we would look at that and say, OK, here is what we use; this is a payment system, this is it. How can we shore this up? How can we make it better?

And we are also working with the vendors that supply. That's a key issue because we're saying, look, we find these things; how can we work together to fix them. And fix them when? Immediately, if not sooner. So we are looking at—I don't think there is—at this stage of the game, there is no, shall we say, holding back of information that would be critical in any instance.

Mr. HORN. What Federal organizations do you coordinate with now? And do you have any suggestions to improve this coordination? For example, the proposed Department of Homeland Security, will that affect this coordination or will that improve it, as you look at the puzzle?

Mr. JAROCKI. I sincerely hope it improves it, and I think it's the right direction, because it's going to focus a lot of the separate efforts that are taking place today. If you took a look at the entire catalog of information that we analyze and collect at the FS-ISAC, it is over 100 different sources. That's not saying it's all Federal, but there is over 100 different sources. And I think, as you suddenly focus it all and bring it together so we have one point of contact, much like we have done with Ron Dick—I mean, one of the good things that we managed to put together was how do we formalize what we do. Where are the points of contacts? How can we get information together? And, how can we hold—a simple thing like we agreed to call each other once a week and say, hi, anything going on? Because you just forget. You are so busy in business-running that sometimes that phone call is necessary. So I think Homeland Security. And if we—everything we read, though, it keeps changing, though. So I'm just trying to map this on my screen. It's not that easy.

Mr. HORN. I have one more question on this, and then I will yield 10 minutes for Ms. Schakowsky. What are the impediments that

limit additional firms from participating in your Information sharing and Analysis Center?

Mr. JAROCKI. I don't think there's any impediments right now, because we are actually working on opening it up to the entire sector. The only impediment, like anything else, is sheer cost. There is always a dollar associated with providing it. And what we are working toward today is a multitiered system so that at least the most important information, which is the alerts and the vulnerabilities, can be gotten to the first responders, to the executive management thing at the lowest levels, immediately, if not sooner.

Mr. HORN. Thank you. Do you want to add something to that, Mr. Tritak?

Mr. TRITAK. No.

Mr. HORN. OK. Ten minutes for Ms. Schakowsky.

Ms. SCHAKOWSKY. Back to FOIA. Mr. Tritak, you said that the President has wanted a narrowly crafted exemption to FOIA or addition to FOIA. Let me just read to you from the bill that came from the administration.

It says: "information Voluntarily Provided, Section 204. Information provided voluntarily by non-Federal entities or individuals that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism and is or has been in the possession of the Department shall not be subject to section 552 of Title 5, United States Code."

That's the Freedom of Information Act.

"anything that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism will be exempt from the Freedom of Information Act." You could hardly call this a narrow exemption to FOIA.

Now, it has been fleshed out a bit in the Armey bill, but the goal of the administration within this Department was to protect all of this information. Now, how does that jibe with your saying that the President wants a narrow exemption?

Mr. TRITAK. Well, as I said before, I think the idea here is to make it narrowly crafted to deal with very sensitive matters relating to critical infrastructure vulnerabilities. It is not to provide a—basically, a dumping ground for any information related to anything with respect to the infrastructure industry that someone might want to put in there and then claim it's protected under the——

Ms. SCHAKOWSKY. So—now, so the narrowness is as long as you can somehow hook it to infrastructure——

Mr. TRITAK. Vulnerabilities. Yes. Now, look, again, this is a draftsman issue. I take your point. I understand that this is very contentious. All I'm saying is that's precisely the process. You are now in play to fix it if you have a problem with it. I mean, truly. No one—let me tell you, nobody intends this to become a mechanism by which basically people can, you know, foist their responsibilities off by data dumping. No one is trying to create a mechanism by which gross negligence and criminal activity can be buried in the government and therefore it can't be prosecuted or otherwise——

Ms. SCHAKOWSKY. Intention really doesn't matter. Intention really doesn't matter. Depending on how the law is crafted, it could be exactly used for that.

Mr. TRITAK. Sure. But part of it—that's why, as I say, it's the give and take of this process, to make it read what it's supposed to do.

Ms. SCHAKOWSKY. OK. Mr. Dick, I want to get back to your statement, and see if you wanted to reconsider it, the statement you made before the Senate: "if the private sector doesn't think the law is clear, then by definition it isn't clear." What do you mean? And do you want to reconsider?

Mr. DICK. One is, as I talked about a moment ago, we spent a good deal of time with the private sector and their general counsels trying to explain how the exemptions as they currently exist under FOIA will protect the information that is provided to it.

The problem that we run into is that the general counsels for these companies either, (a) don't believe it, or cannot provide to the CEOs absolute assurance that the sensitive information that they would be providing to the government would be protected. And so what, by definition, if it—obviously, we're not being able to convince the private sector that those exemptions are adequate, because we have done it over and over again—you have heard it by the members here, on this panel—that it's still a concern to them. And one of my missions as the director of the Center is to try and promote, as best I can, the partnership with the private sector so that they do share that information so that we can compare threats and vulnerabilities so as to assess the risk to our critical infrastructures. And that's what we are seeking. If there is not clarity there, if there is not our concerns, and if there is a way that Congress can resolve those issues, then we support that.

Ms. SCHAKOWSKY. It's really stunning to me. I mean, if WorldCom or Enron or somebody comes to us and says, well, you know, we really don't think we can provide you that information even though we're—our stock has gone all the way down and we're just not going to provide information—that the U.S. Government should change its laws to accommodate that. It seems to me, if we need the information, then we have laws in place and they should give the information. I would like to——

Mr. DICK. This goes back to the point, though. At this moment in time, this is voluntary information, owned by the private sector, that it has no obligation to share unless it wants to. We can't make them do it.

Ms. SCHAKOWSKY. Right. And at a time of war, at a time where we feel threatened, we are negotiating with them to provide critical information, and changing our laws so that they will feel——

Mr. DICK. This issue was raised before September 11th.

Ms. SCHAKOWSKY. Oh, I know.

Mr. DICK. This has gone on for 4 years.

Ms. SCHAKOWSKY. Oh, I'm well aware. I'm well aware they don't want to provide information to the government that we might need to protect our—the safety and well-being of our citizens. And we are going to accommodate that in ways that I think diminish our ability for citizens to have information that they are rightfully entitled to.

I would like examples of what kind of information that—that you are saying that they don't want to provide us.

Mr. DICK. Well, obviously if I knew what that was—you mean general scope examples? Or—I mean, if I knew what the information was, I would——

Ms. SCHAKOWSKY. All right. Just give us categories of information that we aren't going to get because they are uncomfortable.

Mr. DICK. Well, NOSA has to, you know, defer to Stash and the other people at the table for categories of this. But, for example, the specific vulnerabilities associated with the SCADA systems and the processing systems that they are able to determine. Nobody has attacked them yet. But what my job is is to compare what is the threat out there? Are there people, whether they're hackers or al Qaeda or whoever, looking for the vulnerabilities that have been identified out there?

The second piece of the equation at times is unknown to me. I know that there are people out there looking to attack them, but I don't know what the vulnerability is that they may seek to do that by. And at times the private sector is concerned about if they share it, then it will become public and therefore the bad guys will know it and then attack them.

Ms. SCHAKOWSKY. So there is so little confidence, that at this point in history that people within the government would not have the sense to know what information would be critical to al Qaeda, that they are just not going to provide that information?

Mr. DICK. No. We do know what some of that information is.

Ms. SCHAKOWSKY. No, no. I'm saying that businesses feel that they can't trust you to maintain secrecy around information that will help al Qaeda.

Mr. DICK. Well, I think the issue is not if we know it; it's whether the industry's required to provide it, and whether FOIA, in their opinion—meaning the industry—believes that they can protect it.

Ms. SCHAKOWSKY. That's what I'm saying. They don't believe it. They believe that if they provide information that's critical to terrorists, that this government under its current laws is just going to let that information out.

Mr. DICK. Their concern is that the government—if I understand it correctly, and you should ask them—is that the government could not adequately protect it. That's the advice that I understand being given by the general counsels, and we are trying to work with them to resolve those issues.

Ms. SCHAKOWSKY. And I just want to say that it is precisely because of those concerns that the exemptions to FOIA were crafted. It is precisely for that reason that the Executive order—to make sure, as kind of a backup system, Executive Order 12600 was put in place so that those would be protected. These are precious civil liberties, sunshine laws, that now have come into focus how important it is to have transparency. This is what we preach around the world. And I just am at a loss to see why we should use this moment to sacrifice those protections.

Mr. HORN. I now yield 10 minutes for myself.

Mr. Dick, what efforts should we focus on to improve information sharing and success of the Information Sharing and Analysis Center structure?

Mr. DICK. I think the things that we are doing now, and I think we have been able to demonstrate, at least over the last couple of years, that the government can be trusted; and, in particular, the NIPC can be trusted with that information; that we have been able to demonstrate that with it, we can provide back to them timely actionable information to better provide—better protect their assets.

Frankly, as Stash has indicated, it's just going to take time to build up that trust to make the free flow of information to the point that we can do an even better job than what we are doing today.

Mr. HORN. What changes should we make to the Information Sharing and Analysis Center in the new critical infrastructure protection strategy?

Mr. DICK. I'm sorry? Changes insofar as the strategy itself to enhance information sharing? Is that what you're talking about?

Mr. HORN. Yeah.

Mr. DICK. I really think under the President's proposal, as it was talked about a moment ago, by combining these issues that—or, resources,—that we'll have a much more focused and effective and efficient manner by which to deal with assessing threats and vulnerabilities. I think that there will be a lot of leveraging of capabilities across the government by the merging of some of these agencies under one leadership, and overall should have a very positive effect on our capabilities.

Mr. HORN. How are you assured that you are getting the appropriate intelligence information? And, how will the new Department improve the flow of intelligence information to the National Infrastructure Protection Center?

Mr. DICK. One of the things—I mean, I think we've built some very good partnerships with the other agencies that are in the Center. For example, CIA and NSA and Department of Defense and U.S. Secret Service now has a manager within the Center. I think we have about 22 different agencies represented there. And I think one of the things that it is going to enhance, if I understand the proposal correctly, is that DHS will—you know, the flow of information, the requirement of sharing information on a much broader scale, will be further enhanced. With that comes responsibility and accountability for other people's information.

But at least in the current structure, as I understand it, the ability to look at the big picture will be substantially increased.

Mr. HORN. Do you think the private sector and State and local governments are willing to fund the efforts required to adequately secure our critical infrastructure?

Mr. DICK. I think there is a will there. But in these fiscal times of budget deficits, I think it is going to be difficult for State and local governments to find those resources. But the will is there to do that.

I met just last week with representatives from the State of Florida that are looking at starting a State—or, a State of Florida Critical Infrastructure Protection Center. I know that—participated with Texas in doing a similar type of project. And one of the things we have to ensure—I like to talk about the thousand points of light theory insofar as infrastructure protection. I don't care how many centers there are out there or how many ISACs there are out there

or how many members of InfraGard out there, the point is that they are all interconnected and sharing information so that we truly have the ability to determine what the vulnerabilities are and when some threat is going to attack that vulnerability. So I think there is the will. The funding of it is a different question.

Mr. HORN. Before I get to the General Accounting Office, our research arm—and I haven't forgotten you, Mr. Maifrett, and you've listened to all this. What's your thinking on that?

Mr. MAIFRETT. I think the debate of like information sharing is obviously something that should happen. But I think the even bigger problem is that we don't really have any information to share or any worthwhile information. And basically that is to say that there are—you know, if you want to take SCADA systems or just control systems in general, there's plenty of them out there that do have vulnerabilities. I've actually had access to a few of these types of systems myself. And people—you know, myself and also other researchers of the eEye, we found numerous vulnerabilities in that, in the actual SCADA software themselves, in the actual control software.

And this information, you know, it's slowly getting up to the software developers and whatnot so they can fix these problems, but there needs to be a lot more work actually done on determining what is the vulnerability, you know, why is a certain type of infrastructure site vulnerable, depending on the type of setup that it has, whether it's using commercial off-the-shelf software which has vulnerabilities, or whether it be, once again, the actual SCADA software itself.

And you know, I will say again, I think we really need to work hard on actually—you know, to state the obvious, I think we need to work hard on actually fixing the infrastructure sites themselves. And that is creating, whether it be guidelines that are enforced, kind of like we've had in the health care with HIPAA and whatnot.

But we need to basically get down in the trenches. I think there's—you know, while there's a certain amount of high-level talk that needs to be done, there is even more on a technical level that needs to be discussed and hammered out and, you know, true technical solutions to a technical problem need to be put forth.

Mr. HORN. One of your colleagues on Panel One said generally this—and that's Dr. Thomas—noted that hackers who have the skills to break into a supervisory control and data acquisition system are unlikely to conduct a targeted attack, based upon their ethics.

Mr. MAIFRETT. I think with hackers—I mean, there's so many different kind of classes of hackers, if you will. There is more the typical term "hacker" which is used by the media and just by people in general, which is, you know, the people that are posting on mailing lists about security vulnerabilities and that type of thing and doing research. And I think those type of people, you know, people like myself, I definitely consider myself a hacker.

Yes, we actually—you know, there is the ethic there that you would never do such a thing. At the same time, I know for a fact that there's plenty of foreign governments that do heavily research vulnerabilities and how to actually take control of these types of systems. There's other governments that have SCADA systems

also, for example. And just like our government does a lot of analysis in finding vulnerabilities in these types of systems, although a lot of time that information doesn't kind of bubble up to the surface, you know, there's definitely other countries that are doing the same type of thing. And at the same time, there is definitely hackers that, you know, while they might not necessarily have the ethic, there is a certain dollar value that, when brought up, makes that ethic go away a little bit.

So I definitely think there are people out there that do have the skills and they definitely think that sooner or later they are going to be approached, and it's going to start—you know, these types of attacks are going to take place.

Mr. HORN. About a year and a half ago, I was in Italy when they had reached a wonderful part in their economy. And I happened to mention to the Prime Minister, are you worried about any foreign nation trying to upset your economy? Which is very electronic in many ways. And he said, "We certainly are."

Now, from your background, do you worry about that kind of situation? And do you see that type of thing going on, where a good economy of the free world is under fire?

Mr. MAIFRETT. Yeah. I don't know. I mean, there's a lot of times there's talks like that where it's kind of like the economy as a whole or, you know, the North American power grid as a whole and stuff. And I don't think that you necessarily right now are going to see the type of attack that could be that broad and affect that much. I think it's going to be more targeted attacks.

For example, an attack that takes place and the power for Los Angeles goes off, or something like that. I don't think that it's really something that's so broad for the United States in general. But it obviously shouldn't be discounted that—you know, depending on the number of, you know, hackers that you have working for you and how well you are able to coordinate and things. If you hit a few of the major cities and stuff, it obviously can be just as devastating.

Mr. HORN. You recommended enforcing a set of requirements on the security of sites and companies deemed to be integral parts of the Nation's critical infrastructure. Who do you believe should develop those requirements and who do you believe should enforce them? What are some of the practical limitations in enforcing such requirements?

Mr. MAIFRETT. As far as creating them, obviously the infrastructure companies themselves need to be heavily involved. One of the things I stated in my written testimony, though, is that not just the kind of managers, the more high-level people at the infrastructures, but more of the kind of people in the trenches. You know, I mean, I've sat over dinner with people before that do run the power grids, and they joke about how easy it would be for somebody to, using a dial-up modem, get in and shut down certain things.

And I mean, it's people like that where they—you know, they work at these companies, they understand the technology, and a lot of times they understand what they do need to do to help secure it. And a lot of times, though, that information—it's not easy to

kind of bubble it up to the top where it can actually be used and they can start to enforce this thing.

At the same time, I think there is definitely a lot of researchers, including some of the people on the first panel, that have a very good idea of how these systems work and, you know, the kind of technical mind definitely needs to be there. But at the same time, you know, there is a certain amount of the business aspect to it and stuff. So that all needs to be hammered out.

And as far as enforcing it, you know, I don't know. It's not really my place to say who should be the one enforcing it, you know, just as long as there's—somebody is. And obviously—I think it needs to be somebody at the government level.

Mr. HORN. Well, there is a lot of now State information officers, and you have a real wealth of knowledge in the area, and hopefully they will be working with the various Silicon Valleys—east, west, south, and north—and that might be one way to get at the requirements.

Mr. MAIFRETT. Definitely. And just one other, like, side comment. I'd say one of the other problems with why a lot of the infrastructure ends up being secure—you know, we were talking on the first panel, there was a lot of discussion about hackers and whatnot. And the thing that we have with a lot of just the kind, you know, kind of regular software systems that are out there and used by the public, is there are hackers out there that are testing the software, and they are attempting to break it and find flaws in it and whatnot. And these vulnerabilities do eventually get fixed.

And part of the problem, a lot of the—you know, the kind of control systems and software out there are not really accessible by these types of people, and so they are actually not being tested. And, you know, I mean, the few that we actually have access to that we were able to set up, it was a matter of minutes before finding just, you know, total common vulnerabilities that have been known for a very long time now, and it's very easy.

Mr. HORN. Moving now to Robert Dacey, the Director of the Information Security portion of the U.S. General Accounting Office.

And in your testimony, you mention that a clearly defined strategy is essential to ensure that our national approach is comprehensive and well coordinated. What are the key components that should be included in our national strategy? And I would like to know, from your other colleagues here in Panel Two, what are your comments in response to what they've asked and answered some of these questions?

Mr. DACEY. I think in terms of the strategy, we have indicated for a number of years that this was an important aspect. And, as we released in our report last week, there are over 50 entities directly involved in cyber CIP, let alone some of the physical aspects that are starting to be considered as part of our CIP strategy.

I think the key issues go back to what we have in the testimony; and that is, we need to make sure there are clear roles and responsibilities, and how the relationships between all these organizations work. The proposed Department of Homeland Security would include—at least the President's proposal included six entities that would be transferred, still leaving a large number of entities that

would not be. And it is going to be critical to make sure that there is clear coordination about the efforts involved.

The second major area would be, again, establishing clear objectives and milestones and making sure that there are timeframes in place to address them, as well as performance measures which we have throughout government, with GPRA, found to be a very important aspect in terms of establishing the right performance measures and having a regular reporting process to understand the progress that's being made. And I think earlier on the panel, Mr. Tritak indicated the strategy would address those matters.

Mr. HORN. Thank you. And I would like to thank those that brought you here, both Panels One and Two. And we have to vacate this for another subcommittee.

To my left, your right, Claire Buckles is professional staff, American Political Science Association, congressional fellow. Vice President Cheney was one of those Fellows, and so was I. He's way ahead of every one of us. Back here on the wall is the staff director and chief counsel for the subcommittee, J. Russell George. And with him there is the deputy staff director, Bonnie Heald, and they all had a hand in this. And our assistant to the subcommittee, Chris Barkley, is very—standing up in the door there. And we have a lot of interns: Sterling Bentley—is she here—and Joey DiSilvio, Freddie Ephraim, Michael Sazonov, and Yigal Kerszenbaum.

And then for Ms. Schakowsky, we have a longtime professional staff member who knows what he is talking about, one David McMillen. And Jean Gosa, minority clerk, another great institution. And, last but not least, our two wonderful court reporters, and that's Desirae Jura, and Nancy O'Rourke. Thank you very much. And, with that, we are adjourned.

[Whereupon, at 1:05 p.m., the subcommittee was adjourned.]

○