S. Hrg. 107–258

CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE?

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

OCTOBER 4, 2001

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
77–434 PDF WASHINGTON : 2002

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

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

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

FRED THOMPSON, Tennessee
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
GEORGE V. VOINOVICH, Ohio
PETE V. DOMENICI, New Mexico
THAD COCHRAN, Mississippi
ROBERT F. BENNETT, Utah
JIM BUNNING, Kentucky

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
KIERSTEN TODT COON, *Professional Staff Member*
HANNAH S. SISTARE, *Minority Staff Director and Counsel*
ELLEN B. BROWN, *Minority Senior Counsel*
ROBERT J. SHEA, *Minority Counsel*
MORGAN P. MUCHNICK, *Minority Professional Staff Member*
DARLA D. CASSELL, *Chief Clerk*

CONTENTS

WITNESSES

Thursday, October 4, 2001

Alphabetical List of Witnesses

CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE?

THURSDAY, OCTOBER 4, 2001

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

The Committee met, pursuant to notice, at 9:35 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Max Cleland, presiding.

Members present: Senators Cleland, Carnahan, Thompson, Collins, Bennett, Voinovich, and Dominici.

OPENING STATEMENT OF SENATOR CLELAND

Senator CLELAND [presiding]. At the request of Senator Lieberman, who must be out of town today to attend a funeral, I am chairing today's hearing on critical infrastructure protection. I appreciate this opportunity to examine who in the public and private sector is responsible for ensuring the protection of our Nation's infrastructure. This is the second hearing held by Senator Lieberman and the Committee in our continuing series on the security of our Nation's critical infrastructure and the vulnerability of the country's financial, transportation, and communications networks, also our utilities, our public health system, law enforcement, and emergency systems, and others. As you can tell infrastructure covers just about everything of value in our country.

Prior to the September 11 terrorist attacks the Governmental Affairs Committee has been actually diligent in its examination of the responsibilities of Federal agency heads for developing and implementing security programs. In fact, the computer security law, enacted during the 106th Congress, requires Federal agencies to upgrade their practices and procedures in order to protect government information systems from cyber attack. However, since the attacks on Washington and New York City, we have learned that there is still much to be done to protect the Nation's critical infrastructure.

The terrorist attacks provide evidence that physical assaults can cause severe disruptions in the service and delivery of goods and products, triggering ripple effects throughout the Nation's economy, and more importantly damaging the faith of the people in the viability of the day-to-day functioning of the country. Nothing affects Americans more than the disruption of the Nation's transportation, communications, banking, finance, and utilities systems. The country's critical infrastructures are growing increasingly complex, relying on computers and computer networks to operate efficiently and reliably.

The growing complexity and the interconnectedness resulting from networking means that a disruption in one win may lead to disruptions in others. Therefore, President Clinton established the President's Commission on Critical Infrastructure Protection in July 1996. In 1997, this organization released its report and recommended that greater cooperation and communication between the private sector and the public sector is needed in order to decrease the vulnerability of the Nation's infrastructures, which led to their President's release of Presidential Decision Directive 63.

In May 1998, President Clinton released this directive, which sets up groups within the Federal Government to develop and implement plans that would protect government-operated infrastructures and calls for a dialogue between government and the private sector to develop a national infrastructure assurance plan that would protect the Nation's critical infrastructures by the year 2003. This Presidential decision memorandum identified 12 areas critical to the functioning of the country: Information and communications; banking and finance; water supply; transportation; emergency law enforcement; emergency fire service; emergency medicine; electric power; oil and gas supply and distribution; law enforcement and internal security; intelligence; foreign affairs; and national defense, just about everything you can think of.

The directive required each Federal agency to secure its own critical infrastructure and to identify a chief officer to assume that responsibility. The directive also established several new offices to oversee and coordinate critical infrastructure protection. One was a national coordinator designated to ensure that a national plan was developed. The coordinator would be supported by a critical infrastructure assurance office, to be located in the Export Administration of the Department of Commerce.

The directive also created a joint FBI and private sector office, the National Infrastructure Protection Center, which serves as a focal point for Federal threat assessment, vulnerability analysis, early-warning capability, law-enforcement investigations and response coordination. NIPC is also the private sector point of contact for information sharing. Finally, the directive recommended that we have the capacity and the capability to detect and respond to cyber attacks while they are in progress. The Federal Computer Incident Response Center gives agencies the tools to detect and respond to such attacks, and it coordinates response and detection information.

We are fortunate today to have several witnesses who will present their views on the status of the Nation's critical infrastructures, and offer their recommendations on protecting public and private systems from outside attacks.

Senator Thompson, would you like to make any opening remarks.

OPENING STATEMENT OF SENATOR THOMPSON

Senator THOMPSON. Thank you, Mr. Chairman, just very briefly. I think this is certainly a timely hearing. I think we all appreciate now the vulnerability that we have had for a long time, and one that we have discussed in this Committee and others on very many occasions, certainly including cyber security and the problems we have with computer security, and so forth. Of course, that was the background for Senator Lieberman and I introducing the Government Information Security Act.

I think that we are now looking at all these threats through different glasses. Today we are probably going to emphasize, perhaps, one particular issue a little more than others, and that is the cyber threat. Now we are all familiar, all of a sudden, with the threats of biological elements, chemical, certainly nuclear, certainly conventional combinations of all the above, and in addition to that is the cyber threat, which many people think would precede any major conflict that we had with a major power.

Of course, we now know that in this modern age of technology, you do not need to have a major nation-state or a national power in order to create grave problems for us. So now that we have our attention focused after all this time, we are thinking about rearranging the boxes again and creating new laws and new offices, and trying to fit all the stuff that is out there together. Of course, Governor Ridge's appointment, I think, is a good step. But within his bailiwick, as I understand it, will be an Office of Cyber Security.

You have Presidential Decision Directive 63, which addressed the same general problem of cyber security. The GAO has indicated that has not done very well, in terms of what it was designed to do and the offices that it set up. Now we have a new proposed executive order that is not with us yet that will address all of this. We have got the question of what is OMB's role going to be in all of this, since they have responsibility for computer security, and then we have got to ask ourselves how does all this relate to the private sector, as Senator Bennett spent a lot of time on and has legislation on, because we know that most of our critical infrastructure is basically in private hands.

So we have got real big organizational issues on the table to deal with. To me, I think it gets down to a pretty simple proposition, it is going to require leadership, authority at the top, and leadership, and accountability. Maybe we can learn from our past experience with other government agencies and other crises and things of that nature, and not make the same mistakes as we go about trying to rearrange these boxes and decide who reports to who and who has what authority.

Maybe we will take the lessons we learned from our other management problems. In particular, the government basically cannot manage large projects very well. We are told time and time and time again by GAO, by the inspectors general, all the reports that we have seen in terms of our problems with regard to financial management. For example, billions and billions of dollars in waste, fraud, and abuse.

We are told that we cannot manage large information systems. We have spent billions and billions of dollars, money down the drain basically, in trying to get computers to talk to one another. This is a government-wide problem and we think that we are going to come in here and efficiently set this particular thing up and it is going to work well, when nothing else—well, that is an overstatement, of course—but so many things are producing billions of dollars of waste, fraud, and abuse every year. The same agencies come before us every year on the high-risk list, subject to waste, fraud, and abuse, for a decade, but we are going to pull this out and set the boxes right, and then go on about our business the way we did before; we have solved that problem. Well, it isn't going to happen that way unless we have what we have been lacking for years and years and years, and that is leadership from the top on these issues, with the right person having the right authority, and accountability when it does not work.

We are very good at setting up plans and goals, and terrible at implementing them. So I do not want to start out this optimistic exercise on a sour note, but I think it is important to understand that we have got a bigger job than probably what we realize in trying to cut through this morass that we always find ourselves in when we try to solve a problem. And it is especially important here because of the nature of the problem. So, hopefully, today we can get some ideas as to who ought to do what, where the responsibility lies.

I defy anybody to tell us today where the responsibility lies for any of this, but maybe we can talk about where it should lie and where we should go, the direction we should go in, and I think for that reason it will be a useful exercise.

Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Senator Thompson. We will allow everyone to make an opening statement, if they wish.

Senator Carnahan, would you like to make an opening statement?

OPENING STATEMENT OF SENATOR CARNAHAN

Senator CARNAHAN. Thank you, Mr. Chairman. Terrorists did not want to bring down just our buildings. They wanted to bring down our economy. They wanted to bring down our military and our financial and political infrastructure as well. Our losses are incalculable and far-reaching. Still we must face a stark reality: It could have been worse. Now this Congress, alongside the President, must take the lead to ensure we are prepared for the future. I applaud the Chairman for addressing these issues with this series of hearings. When we talk about critical infrastructure, we are talking about American families and their ability to have a quality life.

This means freedom to travel; it means freedom to make a living; and it means freedom to conduct business without fear of terrorism. It means having the peace of mind that your government is doing all that it can to protect you and your children. Grim experience has taught us that terrorist attacks know no boundaries. The ripple effect is extensive. The emotional trauma is long-lasting, and the economic impact is real and widespread. We are all affected, and all of us must be part of the Nation's defense against further attacks.

As the witnesses will discuss today, there are difficulties in creating a unified system to protect our national infrastructure, because control of the different components rests with different entities. On the most basic level, there is a division between what the government owns and operates versus what the private sector owns and operates, but the issue is really much more complex. We live in a global, computerized, and interconnected world. Technological changes have led to great opportunities for human progress, but they have also created vulnerabilities that did not exist even 5 years ago.

Securing our critical infrastructure from cyber attacks, which could be launched from anywhere, is a tremendous challenge for both government and industry. I look forward to hearing from the witnesses today and learning from their expertise. I want to hear their suggestions on what more needs to be done. The question being raised today, who is in charge of protecting our national infrastructure, needs to be answered as soon as possible. We cannot afford to wait for another attack.

Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Senator Carnahan. Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you very much, Mr. Chairman, for convening this important hearing. It would be hard to imagine a more current topic for a hearing than the one that we have before us today on the question of who is in charge of protecting the critical infrastructure of our Nation. Until the terrorist attacks of September 11, in fact, most Americans probably never fully realized the importance of this issue. Tragically, however our eyes are all too open now.

As I have talked with my constituents throughout Maine during the past 2½ weeks, the question of our vulnerability to attack—to various kinds of attacks—and who is in charge and who is coordinating it all has come up repeatedly. This morning, I did early morning radio, back in Maine, and one of the questions was who is coordinating if we have a biological or chemical attack? Another constituent asked me what about our ports? What about if we have a big tanker that is full of liquefied gas coming in? What about the computer systems that are so critical to our commerce and to our government?

The answer to the question of who is in charge seems to be, "Nobody is quite sure." Less than 2 weeks ago, this Committee heard compelling testimony from the distinguished chairmen of two commissions appointed to study this Nation's security, former Senators Gary Hart and Warren Rudman, and Governor James Gilmore of Virginia eloquently expressed their unanimous, but unfortunate, conclusion that, as a Nation, we are simply not properly prepared to defend our critical resources.

If we were poorly prepared for the challenges we thought we faced before the terrible events of September 11, we must surely realize that we are woefully unready now. It seems clear that the protection of our critical infrastructure still consists largely of a smorgasbord of independently-run and poorly-coordinated programs across the breadth of the Federal system. President Bush took an important step when he took office in focusing the National Security Council upon terrorism issues and appointing Vice President Cheney to head a task force to develop better ways to respond to catastrophic disasters.

As the Hart-Rudman Commission and the Gilmore Commission made clear, however, and as recent events have so tragically underlined, it is necessary to do even more. We, in America, have long been blessed by being spared most of the traumas of terrorist attacks that became far too familiar to Europeans in the 1970's, and have been a tragic part of Israeli life for decades. It should be clear, however, that we can no longer afford to attempt to protect our critical infrastructures without clear lines of authority and accountability, and without being able to answer readily and precisely the question of who is in charge.

The difficult, but crucial question now, of course, is who should be in charge and of what? In other words, we must ask who should be in charge at what level, with what specific responsibilities and resources, and with what means of ensuring accountability? And that is why I believe this series of hearings is such an important contribution to the national dialogue of protecting our infrastructure and of winning the battle against terrorism. I am very eager to hear the testimony of our witnesses today, and I want to thank the Chairman and the Ranking Member for their leadership on this issue. Thank you, Mr. Chairman.

Senator CLELAND. Thank you very much, Senator Collins. Senator Bennett.

OPENING STATEMENT OF SENATOR BENNETT

Senator BENNETT. Thank you, Mr. Chairman. I appreciate the hearing and I appreciate the opportunity for us to examine these issues, and the point I want to make with respect to the challenge that we face is that it is seamless. The networks do not begin and end at any particularly defined place. But the efficiency that comes out of the information revolution that we live in has brought with it an increased vulnerability, and the two are two sides of the same coin.

If you go back in American history to George Washington's time, there was little or no connection, let us say, between Charleston and Boston, between Virginia and Massachusetts, or New York, whatever. It was a 7-day journey to travel from one major metropolitan area, if you could call it that, to another. Today, we go around the world with information, money, deals, negotiations, etc., literately with the speed of light. There are no boundaries in today's economy. The borderless economy is a reality, and those who want to take down the Americans who are the best at playing this particular game have vulnerabilities virtually everywhere in the system.

The seamlessness is part of our efficiency. It is also part of our vulnerability, and I got introduced to this whole thing when we got into the Y2K issue and discovered that seamlessness, for me, for the first time. I am interested that the emergency people in New York, who handled all the difficulties after the World Trade Center was hit, have said to Senator Dodd, who has repeated it to me, we could not have handled this emergency if we had not done the remediation required with respect to Y2K.

Prior to the Y2K remediation, they were in the stovepipe mentality, a computer here, a computer there, a system someplace else. Y2K caused them to look at it in horizontal terms, and they praised Senator Dodd for his work, I think appropriately, on Y2K awareness and remediation, because it addressed this problem. We are now, in the terrorist world, simply looking at a situation where this same vulnerability that we identified with Y2K, if the computer should fail by accident, now what do we do if the computers fail on purpose, not our purpose, but somebody else's purpose who wants to break into this infrastructure and cripple us?

So we need to do what we did with respect to Y2K, address the stovepipes, look at this in a strategic manner and say how is the entire system to be protected? As Senator Thompson has said, the majority of the ownership of the entire system is in private hands, not government hands, which is why I have introduced a bill to increase the flow of information between the government and the private sector, back and forth, so that each one can understand in this seamless situation what is going on in their particular part of the world.

So I think homeland security and critical infrastructure protection can come down to two words: Interagency coordination. Now, if that sounds too bureaucratic, think of interagency as including private agencies, but coordination of information, coordination of protection activities, coordination of understanding so that we do not go around with the attitude, "Well, there is no hole in my end of the boat, so I do not need to worry about sinking." With this boat, a hole anywhere hurts us all, and this is an issue that is going to be with us for a long, long time. We are just beginning to understand it. That is why this hearing and others like it are very worthwhile, because it adds to this continually-building layer of understanding, awareness, and, we hope, solutions to this problem.

We cannot go back. We cannot say, "Let us leave the computer age and go back to paper and dial telephones." We are in the Internet age. We are in the electronic age, whether we want to be or not, and we simply have to learn to live with that new vulnerability. Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Senator Bennett. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Mr. Chairman. I thank Chairman Lieberman for calling this hearing this morning, and although he is not able to be with us, we are in good hands with our Chairman pro tem. Today's hearing focuses on the protection of our Nation's infrastructure, an aspect of our society that most Americans tend to take for granted. America's water and sewer systems, computer, roads and bridges, and banking networks, they are all things that most Americans use on a daily basis, but rarely give more than a passing thought.

The events of September 11, however, have changed our way of thinking forever. Americans are now actually aware of how vulnerable our infrastructure systems and physical surroundings can be. That is why it is so critical that we work to protect that infrastructure. This hearing will give us an opportunity to examine how we allocate the responsibility of getting the job done. I would like to just say at this time, Mr. Chairman, that we are having all of these hearings about the various threats we face, but we are not discussing the human capital crisis confronting the Federal Government, which is also a threat. Our witnesses will be talking to us today about all kinds of things that need to be done, but the real issue is, do you have the people in your respective agencies with the qualifications that you need to get the job done?

From my observation of studying this human capital crisis for the last 2 years, we are in very bad shape today. Many people are unaware of the fact that by 2005, about 80 percent of our Senior Executive Service can retire. Van Harp, a senior FBI agent here in Washington who used to live and work in Cleveland told me that, "I'm running my shop with people that are ready to go out the door." And so as we talk about all of these things that need to be undertaken, Mr. Chairman, we had better be aware of the fact that our No. 1 threat is the crisis that we have in our human capital.

As a former Mayor and Governor, I am very much aware of the water, sewers, and other infrastructure that we have in this country. I have to say that even without terrorists, our sewer and water systems in this country are vulnerable because of aging. With the new mandates coming out of Washington today, in my State, for example, sewer rates, and water rates are going up 100 percent. If we are going to do some of the things that we are talking about to protect them, it is going to be costly. And it seems to me, Mr. Chairman, that one of the things that is missing here in Washington today is that we are not prioritizing the expenditure of dollars.

Some of the things that I think are high on people's agenda in terms of spending are much less important than some of the infrastructure needs that we confront here in our Nation.

So I will be very interested to hear from you in terms of the cyber problem. I would say this: I remember how worried we were about Y2K. Do you remember? And we were wringing our hands and we were worried, could we get the job done and is everything going to fall apart? Senator Bennett, who is very familiar with this area, was very much involved in that, but we got the job done, didn't we? But we did not get it done without making it a major priority in terms of personnel and the expenditure of money, and that is what it is going to take if we are going to protect our infrastructure from this new threat of terrorism.

Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Senator Voinovich. Wonderful comments by all the Members of the Committee here. Thank you very much for your participation. I will say as a member of the Armed Services Committee, 1 week before the attacks, as we were marking up the defense authorization bill, I personally asked Senator Pat Roberts, who had been the Chairman of the Emerging Threat Subcommittee, and Senator Mary Landrieu, who is now the Chairman of the Emerging Threat Subcommittee, what they thought was the most probable attack on the United States, where we were most vulnerable. Both agreed that No. 1—a terrorist attack below the radar screen, stealth in nature, either biological or chemical, primarily biological and then cyber attack.

So on the Armed Services Committee, we have been gathering data and information for at least a couple of years now that certainly point to a cyber attack as one of the top two or three attacks that could come via terrorist means on this country.

We would like to welcome all of you. Today's first panel consists of public sector witnesses who represent three of the primary offices created by the Presidential directive. The Committee will hear from John Tritak, Director of the Critical Infrastructure Assurance Office in the Bureau of Export Administration at the U.S. Department of Commerce; Ronald Dick, Director of the National Infrastructure Protection Center; and Sallie McDonald, Director of the Federal Computer Incident Response Center.

Thank you all for joining us here. Before you begin, just some rules of the road here. Just let me mention to you that your full statement will be entered into the hearing record. You can have an opportunity to make a short statement and you will be subject to a time limit, according to Committee rules. Once the light turns from green to yellow, you will have about a minute to wrap up before the red light appears. If you do not stop then, we will make you an air marshal out at National. Thank you for coming.

Tell us a little bit about youselves, and what you do, and some of your thoughts on the subject. But, before I turn you loose, let me just say I have been here in the Senate almost a full term now and on this Committee for well over 5 years. I had no idea you all existed. So please tell us who you are and where you came from and what you do.

Mr. Tritak, do you want to start off?

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

Mr. TRITAK. Thank you, Senator, Chairman, and Members of the Committee. I welcome this opportunity, truly, to be here before you. We generally feel obligated to say that we applaud your leadership on various issues. It is almost a canonical thing you need to say, but, in this case it is absolutely true. I want to add to the remark that was made earlier that this hearing, in fact, was supposed to happen before the attack—it was scheduled before the attack, and underscores the fact that this Committee recognizes there is a real need to address the challenges to our critical infrastructures.

As was indicated in the opening remarks by a number of Senators, we basically have been guided by PDD 63 for about 3 years, and that Directive was created based on recommendations of an interagency group as well as a Presidential commission. Jamie Gorelick, who will be appearing in the next panel, was actually leading that interagency process. So this goes back to the mid-1990's, in terms of the concerns. It created, as you indicated, three organizations, a number of organizations; myself at CIAO, Ron Dick over at the FBI, and Sallie McDonald over at FedCIRC. Needless to say, after 3 years, we were ripe for review, a thorough review in terms of the policies that were established under PDD 63, and frankly, to take a look at the organizational setup of the Federal Government to determine where fixes and improvements could be made.

After 3 years of experience and being in the trenches, if we could not come up with improvements, we really are not doing our job. And President Bush said as much in May of this year, in which he

[1] The prepared statement of Mr. Tritak appears in the Appendix on page 42.

directed that the critical infrastructure policy be thoroughly reviewed with a view towards figuring out ways to improve the organization of the Federal Government to better deal with and address the concerns of this issue, which are extremely complex, as you have all indicated.

He also announced that he wanted, under the directorship of my office, the Critical Infrastructure Assurance Office, to begin to prepare a national plan or strategy to be developed with industry, to develop a consensus in this country, through a document that would be used to inform and make aware and educate on what the problems of critical infrastructure are and what the respective roles and responsibilities of government and industry are in addressing the problem. We all speak about this as a critical infrastructure protection program. If I had it my way, I would strike the word "protection" and say it is critical infrastructure "assurance"—for the simple reason that what we are really worried about here is the assured delivery of vital services over our Nation's critical infrastructures. Those services are provided by both physical- and cyber-based assets.

Increasingly, those infrastructures are being restructured and are increasingly dependent upon information systems and networks—not just to support their business, but to operate their assets. They are also becoming more interdependent, so that disruptions in one sector can actually affect other sectors, as well. What we learned about September 11, if nothing else, is now there are at least some groups whose purpose and goal is to undermine our way of life. They will exploit vulnerabilities wherever they can find them. We had some horrific examples of that back on September 11. I suspect they are not going to stop there.

If they can find and exploit the vulnerabilities of cyberspace, they are going to do so. So it is incumbent upon our government to deal with that problem and work closely with private industry in order to do it. As indicated before, President Bush had inaugurated a thorough review of government structure and government policy, and frankly, we were very close to completing that. In fact, at the time that the original hearing was going to take place we were close to finishing that review. Then the horrific events of September 11 intervened—and what we are working on now, and I expect that the review will be completed fairly soon, is recognition that this is not just about infrastructure protection, it is about homeland security, of which the infrastructures themselves are but a component part.

So what we are trying to do now is identify how and in what ways we can improve, both organizationally and in policy, to address the new issues when, in fact—and I will be quite candid, since one of the roles of my office is to raise awareness, to draw the various sectors together and identify common problems across those sectors to involve other sectors of the economy, like the risk management community, the insurers, the auditing community, the people who influence the corporate leaders—is that we had to emphasize the business case as a way of moving forward. The national security case, in many cases, but not all, but many cases, is simply not self-executing in the market.

It seemed too remote to affect day-to-day business decisions and investments in security. That is not to say people did not take it seriously, but they had to be able to justify those kinds of expenditures against their bottom line—and shareholders and investors who have a whole lot of other things on their minds. Well, September 11 has just frankly changed all of that. I do not think anyone doubts anymore what the needs and importance of investing in infrastructure security, and particularly taking into account now what needs to be done that was not done before September 11 when we got our wake-up call.

So I would say that one of our jobs at the CIAO is to work toward developing a national strategy, working with Ron Dick, who is the operational side of PDD 63—with my organization learning more about the policy-support side—is to address those issues. And what I expect to happen in the fairly near term is for the President to be able to provide a much more comprehensive statement about how homeland security will be prosecuted and how the critical infrastructure dimension of that fits into this overall effort.

Thank you for the opportunity to appear here today, Senator, and I look forward to your comments.

Senator CLELAND. Thank you, Mr. Tritak.

Mr. Dick, tell us a little bit about youself, and what you do.

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

Mr. DICK. Good morning, Senator Cleland and other Members of the Committee. Thank you for this opportunity to discuss our government's important and continuing challenges with respect to critical infrastructure protection. In my written statement I address our role in protecting the Nation's critical infrastructures and how we coordinate with other organizations, both public and private. Last week, while appearing before a subcommittee of House Government Reform, I heard compelling testimony from Mark Seton, who is the vice president with the New York Mercantile Exchange and an eyewitness to the attacks on the World Trade Center.

Although the computer systems and records of the exchange survived the attack, their communications, transportation, and power systems were devastated. Working through contacts in their emergency plans, the exchange opened 3 days after the attack, helping to stabilize energy markets both here and abroad. In this case, diesel generators provided the power, boats provided the transportation, law-enforcement officials and first-responders provided the secure environment. The telephone company provided new lines. His experience proves three things: How our Nation's various infrastructures are interdependent and vulnerable; how an entity that organizes for an emergency and plans for redundancy can operationally survive a major attack; and how the private sector, working with Federal, State and local agencies, can succeed in mitigating the damage in a time of crisis.

The mission of the NIPC is to deter and prevent malicious acts by detecting, warning of, responding to, and investigating threats

[1] The prepared statement of Mr. Dick appears in the Appendix on page 52.

to our critical infrastructures. It is the only organization in the Federal Government with such a comprehensive national infrastructure protection mission. The NIPC gathers together under one roof representatives from, among others, the law enforcement, intelligence and defense communities, which collectively provide a unique analytical deterrent and response perspective to threat and incident information obtained from investigations, intelligence collection, foreign liaison, and private sector cooperation.

This perspective ensures that no single community addresses threats to critical infrastructures in a vacuum; rather all information is examined from a multidisciplinary perspective for potential impact as a security, defense, counterintelligence, terrorist, or law-enforcement manner, and an appropriate response that reflects these issues is coordinated by decisionmakers. While developing our infrastructure protection capabilities, the NIPC has held firm to two basic tenets that grew from the extensive study of the President's Commission on Critical Infrastructure Protection.

First, the government can only respond effectively to threats by focusing on protecting assets against attack while simultaneously identifying and responding to those who nonetheless would attempt or succeed in launching those attacks; and second, the government can only help protect the Nation's most critical infrastructures by building and promoting a coalition of trust; one, amongst all government agencies; two, between the government and the private sector; three, amongst the different business interests within the private sector itself; and, four, in concert with the greater international community.

Therefore, the NIPC has focused on developing its capacity to warn, prevent, respond to, investigate, and build partnerships all at the same time. As our techniques continue to mature and our trusted partnerships gel, we will continue to experience ever-better results. Presidential Decision Directive 63 commanded the National Infrastructure Protection Center to "provide a national focal point for gathering information on threats to the infrastructures." Additionally, pursuant to this 1998 Directive, the NIPC provides "the principle means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts." In the 3 years since that mandate, the NIPC has established an unprecedented level of cooperation among various Federal and local agencies in the private sector.

This cooperation was achieved because we have seen the success of joint multi-agency operations when all members of the intelligence, defense, law enforcement, and other critical infrastructure agencies, as well as our private sector counterparts, combine their widely-varied skills and specialties toward a single goal. The eight infrastructures set forth in PDD 63 have recognized that although they are independent, they are also interdependent and that they must work together in order to reduce or eliminate their own vulnerabilities, and the impact one infrastructure may have on another.

The center has full-time representation from the defense agencies, numerous other Federal agencies, and the Critical Infrastructure Assurance Office. We work closely with the Federal Computer

Incident Response Center, as well as the Joint Task Force for Computer Network Operations at Department of Defense, and other entities which respond to critical infrastructure events. Beyond this and moreover, we recognize the need for a military public-private sector partnership similar to that in the days of World War II.

We in the National Infrastructure Protection Center continue to partner with and support lead agencies, such as the FBI and the Department of Defense. We continue to provide timely and credible warning information to law enforcement, counterintelligence, and counterterrorism, and support to all of our partners in order to fully perform this vital mission. The center is proud to work with your Committee and the Executive Branch to ensure that freedom continues to ring across this Nation.

Thank you very much.

Senator CLELAND. Thank you very much, Mr. Dick. Ms. McDonald.

TESTIMONY OF SALLIE McDONALD,[1] ASSISTANT COMMISSIONER, OFFICE OF INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION, U.S. GENERAL SERVICES ADMINISTRATION

Ms. MCDONALD. Thank you and good morning, Mr. Chairman and Members of the Committee. On behalf of the Federal Technology Service of the General Services Administration, let me thank you for this opportunity to appear before you to discuss our role in critical infrastructure protection. FedCIRC is a component of GSA's Federal Technology Service and it is the central coordination facility for dealing with computer security-related incidents within the civilian agencies of the U.S. Government. Our role is to assist those agencies with the containment of security incidents and to aid them with the recovery process. This directly supports a critical infrastructure protection mission because the Federal Government's agencies depend upon their computer systems, not only to conduct government operations, but also to provide final connectivity to the owners and operators of the Nation's critical infrastructures.

Incidents involving new vulnerabilities or previously unseen exploits require in-depth analysis. Effective incident analysis is a collaborative effort. Data is collected from multiple sources, then verified, correlated and analyzed to determine the potential for proliferation and damage. This collaborative effort has resulted in the development of an incident response community that includes FedCIRC, the NIPC, the National Security Agency, the Department of Defense, the intelligence community, industry, academia, and individual incident response components within Federal agencies.

Though the respective missions of these organizations vary in scope and responsibility, this virtual network enables the Federal Government to capitalize on each organization's strategic positioning within the national infrastructure, and on each organization's unique access to a variety of information sources. Each entity has a different but mutually supportive mission and focus, which

[1] The prepared statement of Ms. McDonald appears in the Appendix on page 61.

enables the critical infrastructure protection community to simultaneously obtain information from and provide assistance to the private sector, Federal agencies, the intelligence community, the law-enforcement community, the Department of Defense, and to academia.

The unified response to recent threats to the cyber infrastructure, including the Code Red worm and the Nimbda worm, clearly demonstrate how these collaborative relationships work and how each participant's contributions help to assess and mitigate potential damage. In both instances, industry alerted the incident response community to the new exploit. During a previous event, a collaborative communication network had been established among numerous government agencies including FedCIRC, the NIPC and the Critical Infrastructure Assurance Office, in addition to academia, industry, software vendors, antivirus engineers and security professionals.

This network enabled participants to share details as they performed analyses and developed remediation processes and consensus for protection strategies. In the case of Code Red, through the collaboration of the above-named groups, the collective team concluded that this worm had the potential to pose a threat to the Internet's ability to function. An unprecedented public awareness campaign ensued concurrent with efforts to ensure that all vulnerable servers were protected. Statistical information provided by software vendors indicated an unprecedented rush by users to obtain security patches and software updates addressing the vulnerabilities. As a result, the impact of Code Red and its variants was significantly mitigated and serious impact to Internet performance was avoided.

Mr. Chairman, the information presented today highlights the critical and effective relationship that exists between FedCIRC and other members of the critical infrastructure community. Though each contributes individually to critical infrastructure protection, our strength in protecting information systems government-wide lies in our collaborative and coordinated efforts. I trust that you will derive from my remarks an understanding of the cyber threat and response issues, and also an appreciation for the joint commitment to infrastructure protection of FedCIRC and the other members of the critical infrastructure community.

We appreciate your leadership and that of the Committee for helping us achieve our goals and allowing us to share information that we feel is crucial to the protection of our Nation's technology resources. Thank you.

Senator CLELAND. Thank you very much, Ms. McDonald. We will open it up in a minute for a round of questions. Each Senator will have 8 minutes in order to delve into some of these questions that plague our country. One of the things that occurs to me on this particular point of vulnerability to cyber warfare is a question that I ask myself about the intelligence community, but what comes to mind is that line by a humorist in Georgia, now deceased, Lewis Grizzard, who once said that life is like a dog sled team. If you ain't the lead dog, the scenery never changes. I am looking for the lead dog. Who is the lead dog among you here? Is there one? And is that a problem?

In other words, it is interesting, Mr. Dick, you are director of the National Infrastructure Protection Center, FBI. Mr. Tritak, you are the director of the Critical Infrastructure Assurance Office, U.S. Department of Commerce. Ms. McDonald, you are over in the Federal Computer Incident Response Center, GSA.

Do we have a lead dog in the Federal Government that runs the war against cyber terrorism, Mr. Tritak?

Mr. TRITAK. Senator, under PDD 63, the lead person for coordinating government policy on critical infrastructure protection and assurance issues is the National Coordinator for Security, Infrastructure Protection, and Counterterrorism at the National Security Council, and that is Richard Clarke. What they did is create two basically parallel offices; one for operational threat assessment and warning and the like. It is an interagency office that happens to be housed at the FBI. That is Ron Dick's.

The other was a policy, planning and support group with an emphasis on dealing with some of the cross-cutting issues of private industry. So if you ask under the PDD 63 rubric, the person that has front-line responsibility in oversight is Richard Clarke over at the National Security Council. As I tried to indicate before, all this is under review, and what is being considered now is how to not only accomplish what Senator Thompson had indicated, which was to establish the lines of authority, accountability, but, frankly, also what are our policy priorities. If you have the best organizational chart in the world, things won't get done unless the matter is a priority with the backing of the highest guy in the land—the President of the United States.

I think there is no question under the current circumstances—and I do not think it was a question before the circumstances of September 11—that critical infrastructure protection is going to be a priority for this President. But, as things are, the policy review process is ongoing, but being wrapped up and, unfortunately, many of the people who are involved in finalizing the policy review are also very busy actually dealing with the terrorist problem we are confronting at the moment. So if you ask me today: To what extent is PDD 63 still in play? I would say that it is for the interim, but I would also tell you that is going to change very soon.

Senator CLELAND. Mr. Dick, any comments?

Mr. DICK. No, I completely agree with John's comments as to who is in charge—that is according to the guidelines under which we exist today and which are under review. I would like to make one quick comment in agreement with Senator Bennett. No matter who is in charge, the key to success that we have found is the building of interagency cooperation to include the private sector. We in the center, as I said, have been in existence for about 3 years. We have had a number of initiatives. One is called InfraGuard, a grassroots effort with security professionals in both cyber and the physical world, to share information.

We currently have about 2,000 members throughout the country. We have chapters in every one of our 56 field offices at the FBI and even a few more cities across the Nation. We are working very closely with the information sharing and analysis centers that are formed within the private sector for banking and finance and electrical power and water, and we are working very closely, obviously, with our partners in the Federal Government to share information, and succeeding in getting cooperation in that. But the key to that interagency cooperation is the building of one word, as I said in my statement, trust.

Trust takes time, but trust is evolving. I think the things we have seen that Sallie alluded to, with the Leaves virus, Nimbda, where you saw a combining of law enforcement, intelligence community, private sector individuals coming together, really experts in this field, determining what is the issue, what is the resolution to it and providing to the public a means by which to mitigate and solve the problem, was truly successful. And I think that across all infrastructure protection, as well as homeland security, that is the issue—is what Mr. Bennett alluded to, is the cooperation between all of the agencies.

Senator CLELAND. Can I just underscore that? It does seem, and I hate to inflict another comment on you, but I was thinking about Casey Stengal's great line when he was coach of the Yankees. He said that it is easy to find the players, but it is tough to get them to play together. It does seem to me that the challenge here is the coordination of the existing assets, I mean, step one, and we are all human beings. We all have our offices. We all have our departments. We all have our allegiances. Trusting someone outside that department, outside the framework is the challenge. In other words, building a team may be tougher than just putting some names on an organizational chart.

Mr. DICK. And you are absolutely right and let me, if I may, give you another, what I think, is a very good example. My experience in being involved with the center for over 3 years and being the director for the last 6 months, is that the people I have dealt with in the other agencies, people I have dealt with in the private sector, are all trying to do the right thing. There are no agendas here going on in my opinion. These are people that are legitimately trying to do the right thing and figure that out.

One of the things, I think, is a success from our standpoint is the relationship the center has built up with the Joint Task Force for Computer Network Operations under General Bryant in the Department of Defense. General Bryant and I are in complete agreement about one thing, that I cannot do my job without JTFCNO and the Department of Defense as an integral partner. And General Bryant agrees with that same statement. So we have built, what I think and I think General Bryant does too, a very good working relationship that is built upon trust and sharing information, and that information not being used in a wrongful manner. But that takes time.

Senator CLELAND. Mr. Dick, I would like to observe, too, that we are all trying to do the right thing here, too. If some person on the National Security Council is the lead dog or the top coordinator or the ultimate person to which this information is followed up, that person is not confirmed by the Congress and it is tough for the Congress to be part of the team. In other words, I do not think we have the authority to call up Mr. Clarke and ask him how the war against cyber terrorism is going? I mean, he is on the National Security Council. So that is just a challenge for us here as we try to plug ourselves into our oversight responsibilities.

Ms. McDONALD. Well, I certainly agree with both John and Ron's statements. We have come together as a team, because I think this community, probably more than others, has recognized the vulnerabilities in the cyber area, and recognized, as Dick Clarke frequently says, that there will be an electronic Pearl Harbor. None of us were expecting the events of September 11, and we in the cyber community are hoping not to see anything of that magnitude in this area. But if we do not all come together, if we do not devote resources, if we do not correct the human capital situation that Senator Voinovich addressed, we have a tough job ahead of us and many challenges.

Senator CLELAND. Amen. Well said. Senator Carnahan, any questions?

Senator CARNAHAN. Certainly, all of us would agree that we are going to have to be looking into the types of attacks that we are likely to face, and whether or not we are prepared for them in the public or private sector. The attacks in New York and Washington were targeted attacks. Is our infrastructure equipped to withstand a larger geographical attack on a larger geographical area? I would address that question to Mr. Dick, and also, could you explain how NIPC is preparing for such a scenario, and what steps you are taking to help the private sector prepare for something of that nature?

Mr. DICK. Thank you. Obviously, whether we are prepared for a particular attack depends on how big. Obviously, you can make a threat scenario so large that you eventually lead to—well, everything is shut down, but in taking what would normally be perceived by the intelligence community and us as reasonable threats that are out there, that are potential, that could occur—I think the private sector and the U.S. Government entities, as well as State and locals, are preparing themselves. Are they adequately prepared? No. Like the events of September 11, no one could have predicted, I think, with any great certainty that those things could have occurred.

What has happened, though, in the last few years is a raising of the awareness, if you will, of the need for the contingency plans that I talked about in my statement by Mr. Seton, and with the Mercantile Exchange in New York. Because of those efforts, this particular company took a lot of time and effort to build these contingency plans. Has North American Electrical Liability Council and all the electrical power companies done the kind of contingency planning and consideration of redundancy issues that they should have? Probably not, but I think with heightened awareness and coordinated planning, as Mr. Bennett was talking about, in cooperation with each other, we can achieve a very robust ability to respond and survive almost any kind of attack.

Senator CARNAHAN. Do you feel like you need additional resources or tools to be able to make NIPC more effective in this regard?

Mr. DICK. Well, absolutely. We are moving forward right now. We have submitted a supplemental proposal and we are working it through the Department of Justice and OMB as we speak, to address many of those issues to reach what we are calling full capacity to address these issues as they occur, and it will be through a phased-in approach. But we have made that request already. What

I think is another issue here, and it is not just a matter of funding to the NIPC or funding to the FBI—it is a matter of being able to get the experts in this area, whether it be in the cyber, whether it be in WMD issues, in the private sector, at the table with the government to share what those vulnerabilities are and how those fixes are occurring. So it is not just a personnel issue for governmental entities. It is much broader than that.

Senator CARNAHAN. One final question, Mr. Tritak. Certainly a key component of our country's ability to recover from a terrorist attack is the government's ability to continue functioning. I was wondering if you could discuss what steps are being taken to ensure that the Federal agencies have the capability to continue functioning in the event of an attack, and with whom does this responsibility fall?

Mr. TRITAK. Well, Senator, actually, there is one piece of this I can answer and there is another bit of it that, I think, probably would be better discussed in another environment about the continuity of government and how we ensure you have a fully functioning government under all circumstances. But one thing we are doing under my mandate, under PDD 63, is to assist agencies in identifying the key critical services they provide, identifying the systems that support those service deliveries as a way of mapping potential dependencies and vulnerabilities that they have to address and safeguard.

So for example, and I use this in my written testimony, I think everyone would agree, for example, that a timely warning of a hurricane would be a vital service the government needs to provide. Ensuring that service is deliverable—it is not sufficient simply to make sure that the Tropical Prediction Center in Miami, Florida works. The fact of the matter is, a number of inputs from other government agencies and private sector entities feed into that system. Some of those, if disrupted for even brief periods of time, could actually impair the delivery of vital information that warned of hurricanes with the result in loss of life if it is not brought up quickly.

So one of the things we are all doing in accelerating, and this is, in fact, something that is fully supportive of the efforts that were passed under the Lieberman-Thompson bill of last year, is to accelerate that mapping process within each of the civilian agencies, where we focus on the civilian agencies, because, frankly, the Defense Department, they do this as a matter of course. So in that respect, what we are looking at is ensuring critical government services. In some of those cases they rely on private sector infrastructure service providers to help. We have given these agencies a way of identifying what they have to prioritize and pay attention to to ensure that those services, whether they are Social Security checks, hurricane warnings, or mobilization of U.S. forces to project power overseas can be done.

Senator CARNAHAN. Thank you.

Ms. MCDONALD. Senator Carnahan, if I could add, the General Services Administration is also charged with continuity of government operations. As you probably know, we not only have the Federal Technology Service, which provides long-distance telecommunications service and information technology service, but we also have the Federal Supply Service that has been instrumental in providing supplies both to New York and the Pentagon, and we have the Public Building Service where we provide office space, etc. So we do have contingency plans to reconstitute government as far as buildings, technology, and supplies are concerned.

Senator CARNAHAN. Thank you.

Senator CLELAND. Thank you very much. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman. Mr. Dick, can you tell us how many people are actually doing analysis in your information sharing unit?

Mr. DICK. I think there are 10 or 12 that are FBI employees. I would have to confirm those numbers. From an interagency standpoint, we probably have another four or five. Now, that is just doing analysis. Within the center, we have a total of approximately 90 FBI and 20 interagency folks.

Senator BENNETT. I understand that in November 2000 the FBI director wrote to Sandy Berger complaining that the other Federal agencies did not recognize NIPC's mission, and he said NIPC would not be able to provide analysis and warning, if the NSC did not, in fact, assist NIPC in obtaining personnel. Are you aware of that letter or of that concern and do you share that concern?

Mr. DICK. I am aware of the letter and I share that concern. As I spoke a moment ago, to one of the key factors of the success of being able to provide strategic analysis, is the interagency nature of being able to get many people from different disciplines to look at the same data, and to determine if the vulnerability in the banking and finance sector is applicable to the electrical power sector. And that is one of the findings that was referenced by Mr. Thompson in the GAO report. In fact, my reading of the GAO report was that it said we did investigations pretty well and we did outreach pretty well, because of InfraGuard and some other things, key asset initiatives. It said we did training pretty well. So we did a number of things pretty well.

But what it said we did not do very well was strategic analysis. They said we did not do strategic analysis very well, meaning predictive analysis, because we did not have the resources, both from an FBI standpoint, but more importantly, from an interagency standpoint. And it has been my public position that GAO was right. You know, their conclusion was absolutely correct, but——

Senator BENNETT. It always bothers you when that happens.

Mr. DICK. Yes, it does, but I try to get over it. We have been working very diligently with other partners, and there has been some response from many of the agencies in providing us resources.

Senator BENNETT. That was going to be my next question. Have things gotten any better since November 2000?

Mr. DICK. They have gotten better. The CIA has provided a senior officer to head the analysis and warning section, and it made a commitment for multiple years for that person to be engaged there. He is an excellent person. Behind me here, the Department of Defense has sent over a two-star Rear Admiral from the Navy to be my deputy director for the center, Admiral Plehal. He is working very diligently with the other Department of Defense agencies to fill those gaps that we have talked about before. The

National Security Agency has sent over a senior analyst to head up the analysis and information sharing unit.

So there have been a number of issues that we have made progress on. Are there still gaps? Yes, sir, there still are gaps, but I am seeing greater cooperation, and I think since the events of September 11, there has been an even heightened awareness of the need for participation and sharing of information within the center.

Senator BENNETT. Well, let me ask all of you, you have referred to this collaborative analysis, who has the ultimate responsibility?

Mr. DICK. For production of products?

Senator BENNETT. Yes.

Mr. DICK. Generally, the center is the one that assists in the production of that and coordinates the production of that, along with others, particularly in the private sector, and then pushes those products out. One of the things that you have to keep in mind, a lot of the solutions are not necessarily government solutions.

Senator BENNETT. Oh, I understand that. I am just talking about the analysis here, and you are saying it is focused in the NIPC and the FBI.

Mr. DICK. But it is a collaborative effort, where like—as Sallie was talking about on the Code Red worm, we bring the unique skills that each of us possessed together to look at a particular problem or issue, and then come up with mitigation or a solution. So it is not us in the center alone. It is a partnership with the others, a big partner, private sector, the antivirus community, and the other software vendors.

Senator BENNETT. Yes, and that is what my legislation is trying to address, to increase that partnership with the private sector, but if the Chairman can quote baseball, if I were advising Tom Clancy on his next novel, who would be the official who would go running to the Oval Office and say, "Mr. President, an attack is coming," and our analysis shows this from the private sector creates a pattern that we discover that holds with the Defense Department, and the CIA tells us and so on. Our analysis shows that there is going to be a major incident coming, on the Tom Clancy mode, would that be Dick Clarke who would go forward with that? Would that be the director of the FBI? Would the director of the FBI tell the Attorney General? Who? Who ultimately is the one in whose mind that the alarm bell should go off that, "Hey, this pattern of analysis shows we have a major, major vulnerability here, and it looks like somebody is getting ready to exploit it?"

Mr. DICK. Yes, I think it would be a collaborative effort. Obviously, we are in direct contact with Mr. Clarke and the National Security Council almost on a daily basis because of the events of today. So when you are saying who is going to run and brief the President, those briefings that occur every day with the Attorney General, the director of the FBI, and representatives from the National Security Council. In the kind of event that you are talking about, there are sensors out within the private sector, but also within CIA, NSA, DOD, the FBI, and all of that intelligence is churned together to make those briefings. So I do not know that there is a person that would be running up to the President.

Senator BENNETT. Do you have any expectation, and I realize this is speculation, but let's speculate—do you have any expectation that Governor Ridge will become that person?

Mr. DICK. I have not seen the final—or I have seen a draft of the executive order, but I do not know how that is all going to flesh out.

Senator BENNETT. Either of the other two? Do you have any—

Mr. TRITAK. I will venture a speculation, which hopefully I will not pay for. [Laughter.]

Senator BENNETT. We will protect you.

Mr. TRITAK. I think it is fair to say that just based on administration statements recently, there is going to be someone who will be responsible for this—recognizing there are channels of constant communication on intelligence matters with the FBI and everybody else—there will be somebody who will, in addition, have a responsibility for reporting those sorts of things to the Cabinet and therefore the President. It is a question of who and under what circumstances, and I think that is what is actually being worked out.

I think what is informing your question is the recognized need to ensure is that there is someone with sufficient authority, accountability, and has the ear of the President who is going to be able to communicate these concerns in a timely manner, and I think that there is every effort from what I can tell, just in the various reviews that have been going on at an accelerated pace, that the answer will be yes, there will be someone responsible. What we cannot tell you now is who, for sure.

Senator BENNETT. If I may, Mr. Chairman, I am asking these questions of the administration. If someone were to turn the tables and say who in the Senate would be the one to alert Leader Daschle, we would not have an answer to that on this side of the dais. Thank you very much for your testimony and for your service in this area.

Senator CLELAND. Thank you very much, Senator Bennett. Senator Domenici.

OPENING STATEMENT OF SENATOR DOMENICI

Senator DOMENICI. Thank you, Mr. Chairman. I apologize for being late and I am sorry I did not get to hear whatever you had to say before I arrived.

I just want to make two observations, Mr. Chairman. It would be good to have before us how many meetings we have had of this type, talking about better coordination among the important aspects of the government and the people, so that they know what is happening and what might beset them and their families. Most of those hearings would be drab and dull, and maybe if the Committee had not reported so many bills during the year, it might report one on the subject of coordination, so that we would not just add to another tall list of coordination requirements.

I will not say people in the government will not follow them, but I would suggest there would not be a great deal of urgency about getting them operative, solving problems within the legislation that requires meeting for this and meeting with this leader or that person. I would hope that has ended, and I would hope that you, Mr. Chairman, and the Chairman of the Committee, would consider the subject matter of this hearing something serious enough that within a very reasonable time, it should be achieved.

We should have legislation that does something with reference to this area of infrastructure, organizationally speaking, so as to preserve it and make sure we know what we are doing and others can rely upon what we know. I happen to have a bill that is before us, S. 1407, the Critical Infrastructure Protection Act. It follows in tandem with what we understand the President's proposals are going to be, by way of executive order. I am hopeful that soon, whatever other bills are going to be introduced and considered, that our Chairman will proceed with dispatch to mark up this kind of bill, unless to be effective, we need to do a lot of other bills.

I have not passed judgment on that yet myself, but obviously a very big vacuum existed in terms of communicating to someone about a problem that was going to fall upon our people on that now infamous day, September 11. I compliment you and this Committee, because I think this is not normally very exciting work. But we ought to do something with the smartest people we have and the equipment we are capable of buying and putting in place if we think the problem is serious enough. We surely can do much better than we have done, and we can have in place within a year something much better than we have by way of infrastructure safety, cooperation, and information exchange.

Thank you for what you all do. I am going to wear my other hat, which I am a little bit better known for, the budgeting part, and I am going to go talk about the stimulus. I have already chatted with you, so I kind of know what you think. Maybe we can get something done on that quickly, too, let's hope.

Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Senator Domenici. Thank you for stimulating and underlining the need for increased coordination and cooperation on this vital issue of security, in terms of our cyber world, both public and private, and just to point out and underscore the Senators concern if we cannot get together public entities, private entities, Legislative and Executive Branches—if we cannot get together now, under these circumstances, when will we ever get together? So that is our charge.

We would like to thank the panelists for your time and attention. Thank you very much. We would now like to call the second panel.

We thank you all very much for coming today, and we would like to welcome Frank Cilluffo. He is the senior policy analyst and deputy director for the Global Organized Crime Project, from the well-known and well-respected Center for Strategic and International Studies, which I understand the board of trustees is chaired by my friend, Senator Sam Nunn, from Georgia. You are a senior policy analyst and recently chaired two homeland defense committee hearings on counterterrorism and cyber threats and information security at CSIS. We welcome you today.

Jamie Gorelick, the Vice Chair of Fannie Mae, who, as you know, is a private shareholder-owned company that works to make sure mortgage money is available for people in communities all across America. We welcome you today.

Joseph Nacchio, Chairman and CEO, Qwest Communications, and Vice Chairman of the National Security Telecommunications

Advisory Committee. We would like to learn more about that. Qwest Communications offers local and long distance telephone, wireless, and Internet web hosting services over a state-of-the-art network to homes, businesses and government agencies in the United States and around the world.

Kenneth Watson, President, Partnership for Critical Infrastructure Protection Security, who is very much involved in dealing with these threats and vulnerabilities, countermeasures and best practices within and between industries. We are delighted to welcome all of you here.

May I just throw out a couple of questions here that you can respond to, please? The President has put forward the notion of an Office of Homeland Defense. It is interesting that it has cabinet-level status, and it needs it, and the office will report directly to the President, and I think that is very much needed. However, interestingly enough, the Rudman-Hart Commission that looked for 2 years at the question of American defense focused more and more, because of the testimony they received, on a terrorist attack and concluded that—a year ago, in their report—that it was not a question of whether a terrorist attack would come on this country, but when, and therefore recommended a full-blown agency of homeland defense, in effect with a budget of its own and, in effect, infantry, troops, people at its command, Border Patrol and so forth, the Coast Guard and the like, that could be put into operation in terms of homeland defense.

We just want to let you know that is something that is on my mind as you now have an opportunity to give an opening statement, and we will start off with Ms. Gorelick.

TESTIMONY OF JAMIE S. GORELICK,[1] VICE CHAIR, FANNIE MAE

Ms. GORELICK. Thank you very much, Senator Cleland, and I very much appreciate the opportunity to be here. I testified on this subject, I think, the first time before this Committee in July 1996, and I said at the time that I hope we would not have to see the electronic equivalent of Pearl Harbor before we did something substantial. We have not had an electronic Pearl Harbor, but we have had a Pearl Harbor, and it, I think, puts what we are doing as a country in a different perspective.

As Senator Thompson said just a little while ago, we are seeing things through different glasses. I have a long interest in this issue. I came to the Department of Justice from the Department of Defense. At the Department of Justice, where I served as deputy, I was in a position—not unique, but there are not very many people who see both domestic and foreign intelligence on a daily basis—that caused me to be very concerned about our national infrastructure and the lack of responsibility for protecting it, particularly in the area of cyber security (but also our entire national infrastructure).

We started a Working Group which resulted in a Presidential Commission, which resulted in PDD 63. I have been long interested in these issues. I currently serve on the Director of Central Intel-

[1] The prepared statement of Ms. Gorelick appears in the Appendix on page 70.

ligence National Security Advisory Panel and on President Bush's National Intelligence Review Panel. So I have kept an interest in these things. I am here as Vice Chairman of Fannie Mae, to comment on the readiness of the financial services sector of our economy, but also with this background.

So let me make a couple of comments and see if I can come back to the question that you posed, Senator Cleland. We have realized as a country, for now 5 or 6 years, that we need to have a hardened-against-attack private and public infrastructure. We need to have the comprehensive ability to detect intrusions. We need to have comprehensive planning, warning, and operational response capabilities.

The two original actions that emerged from the Presidential Commission did, as we just heard from the last panel, create two efforts, a law-enforcement effort and an effort to get industry to where it needed to be. There has been progress, but frankly it has not been enough. The events of September 11 serve, if nothing else, as a wake-up call. From the point of view of industry, the original concept was that industry should be encouraged, if you will, to work together to form such things as the Partnership for Critical Infrastructure Security, and various information sharing analytic centers, to work together.

That made sense, because industry asked the Commission not to put in place government command-and-control of industry infrastructure. And there was, as you have heard from the previous panel, a decided lack of trust between industry and government. So the first step was to build trust and each industry was to be encouraged to work together. Various of these information sharing and analysis centers have, in fact, been stood up. I would say to you—and I have submitted my testimony in greater length on this subject—that there is an uneven range of results, uneven participation, uneven robustness of capacity. And in some industries, the effort is still nascent.

These ISACS, by and large, have no funding, no permanent staffing, no real operational capability. So when you point out, Senator, as you have quite appropriately, that 90-plus percent of the information infrastructure on which this country's security rests belong in the private sector, that private sector's organizations to deal with this issue are not, I think, where they need to be. I think now, perhaps with the greater sense of urgency, there will be a greater willingness on the part of industry to step up to the plate and also to accept help from the government.

I think we need a more realistic approach, one in which the government does more to bring industry together for the sharing of information. We need a new legal rubric, and I commend Senator Bennett for addressing the Freedom of Information Act issue and the antitrust issue, both of which will bring greater coordination to and greater flow of information from the private sector to the government. And we need greater clarity on chain of command, if you will, within the governmental structure.

I would say one word about law enforcement. The NIPC is to be commended for the work that it has done. To the question that all of you have asked, the FBI is in charge, under PDD 63; it is very clearly the lead agency. But if you look at the resources that the

FBI in general has had to fight terrorism, compared to the resources that a CINC would have to protect the national interest, say, in the Pacific, it is absolutely dwarfed. There is no relationship between the job and the resources.

The worry that I have about a coordinator in the White House is that we will not get to the point of real homeland security and defense, the way the Defense Department would step up to it if it had that job. I do not know what the thinking is in that regard, since I am not in the government. But I would say to you, having served in both places, there is no one in the government with the operational capacities and the wherewithal of our Defense Department. And unless you get to that level of scale and capacity to protect our national infrastructure, we will, I am afraid, remain at risk.

There is no one currently doing the kind of planning we need done, and there is no capacity, for example, that I am aware of for a military response to a cyber attack on the private sector.

Thank you.

Senator CLELAND. Fascinating testimony, Ms. Gorelick. Thank you very much. Powerful. Mr. Nacchio.

TESTIMONY OF JOSEPH P. NACCHIO,[1] CHAIRMAN AND CHIEF EXECUTIVE OFFICER, QWEST COMMUNICATIONS INTERNATIONAL, INC.

Mr. NACCHIO. Thank you, Mr. Chairman and Members of the Committee for inviting us. It is an honor to be here this morning. Let me begin by first introducing who we are. We are not as well-known as most other big companies. We are a 5-year-old Fortune 100 company. We have 66,000 employees and revenues of about $20 billion. We provide local, long distance, Internet, broadband, and wireless services across the United States and Western Europe, and we own the incumbent local telephone company in 14 Western States. We also provide services to agencies of the U.S. Government, notably the Departments of Defense, Energy, and Treasury.

I am also testifying today, as you noted earlier, in addition to my capacity as Chairman and CEO of Qwest, as the Vice Chairman of the National Security Telecommunication Advisory Committee (NSTAC), and I bring to that organization all of my experience in the industry, about 30 years, and a deep concern on this issue, an issue we have been addressing for the better part of the last 3 years. In cyberspace, we have been at war for 3 years. It is now just catching up to the general consciousness of the country.

We are constantly hit with viruses and almost ironically, the success that the telecommunications industry has had over the last 30 years in defending against physical attacks and nuclear war, has now made us vulnerable in cyberspace. Although we have moved much of the physical layer out of danger, although there is still some danger, we now have cyber defense as one of our biggest issues.

I would tell you though, that instead of focusing just on vulnerability, we should also look at resiliency. And, as the President re-

[1] The prepared statement of Mr. Nacchio appears in the Appendix on page 76.

assured the Nation 2 weeks ago that the state of the Union is strong, I would tell you this morning and assure you that the telecommunications infrastructure of this country is strong.

Our infrastructure and telecommunications is the best in the world. Our engineers, technicians and workers maintain it second to none, and we saw that proof on September 11, because despite the horrific damage at the World Trade Center and at the Pentagon, most of the Nation's telecommunications and Internet infrastructure worked flawlessly at a time of increased demand.

The problems were isolated to the end links in the network. We had wireless overlays in play. It was far better than most people, I think, would have imagined. At ground zero in New York, telecommunications companies put aside their everyday marketplace rivalries, including ourselves. For example, we diverted a multimillion dollar shipment of equipment that was supposed to come to us in the West directly to Verizon, so that we could restore those central offices down on West Street. We worked with FEMA to provide communications between the two critical locations in lower Manhattan the day after the attack, and we provided Internet connections and services to all who had lost them.

Similar efforts were made by other telecom companies. We have a collaborative industry, and in this case, it was praised by FCC Chairman Michael Powell, who quoted it as a heroic act, ensuring the world's premier communications network has continued to be available in times of tragedy. So we should look at both the vulnerabilities and the resiliency of our infrastructure, and understand how resiliency came to pass: It has been through collaborative efforts that have occurred over the last 20 or 30 years.

The telecom industry understands that our networks are quite literally the conduits that connect the world and the essential sectors of the economy, and keeping both our internal and external networks safe is something that the companies in our industry do every day and will continue to do. Let me give you two examples that make this real from our own experience.

First, to defend our internal Qwest physical network from physical and cyber attack we have implemented a comprehensive information network security program which includes classification of the network assets, the implementation of a complete set of security policies and procedures, extensive employee training and a plan for disaster recovery and reacting to disasters.

The NSTAC leadership has broadly circulated the Qwest program, encouraging the other members of NSTAC to implement a similar program.

Second, to protect our external networks, just last month we dedicated 1,000 technical experts to assist our customers affected by the global Code Red computer virus, which penetrated our firewalls and took down our customer networks. Such a quick and comprehensive response is what is necessary across all networks. But doing it in our own networks is not enough. Doing it inside the telecommunications infrastructure is not enough. Other industries need to take similar steps because we are all interconnected in cyberspace.

It is no longer important to just protect your physical layer. You have to protect the software layer. We are all connected. Each company must therefore protect its own network, assets and people, and all companies must coordinate those actions. I have some very specific proposals that I think address this.

First, NSTAC and the National Security Council should immediately initiate a project to develop benchmarks and requirements for information security best practices for the telecommunications industry and its users, because again we are interconnected. Either NSTAC or another public organization, such as the National Infrastructure Simulation and Analysis Center, proposed by Senator Domenici, should be given the responsibility to extend these clearinghouse and coordination functions to other industries and other agencies, as well.

Second, I think Congress should remove the perceived barriers to information sharing. Your legislation, Senator Bennett, with Senator Kyl, is critical to allow us to share information safe and secure, so that the information we are sharing with the government does not fall into the hands of the perpetrators to begin with, under the Freedom of Information Act, and we can collaborate without the threat of antitrust, based upon the national security needs.

Third, and this is very important to us who are fighting this every day, we need legislation increasing the penalties for cyber attacks. This is not a humorous subject for hackers. It has to be a serious subject. It costs money. It costs time. It puts people in vulnerable circumstances when they lose their communications infrastructure. We need to give law enforcement greater latitude to investigate and to prosecute these attacks.

Let me conclude by saying that the telecommunication infrastructure is strong. There is more work to be done, but it can and must be made stronger, and I know that we at Qwest and my colleagues in the communication industry will do whatever is necessary to help this Committee, the Congress and the administration to ensure the continued strength of America's telecommunications infrastructure.

Senator CLELAND. Thank you very much, sir, for that very strong testimony. Mr. Cilluffo.

TESTIMONY OF FRANK J. CILLUFFO,[1] CO-CHAIRMAN, CYBER THREATS TASK FORCE, HOMELAND DEFENSE PROJECT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. CILLUFFO. Mr. Chairman, Senator Bennett, it is a privilege to appear before you today to discuss this important matter. In the wake of the terrorist attacks on the World Trade Center and the Pentagon, the United States is confronted with harsh realities.

Our homeland is vulnerable to physical attack and gone is the sense that two oceans that have historically protected our country can continue to protect Americans. The terrorists attack highly visible symbols, not only of military strength, but also of our economic prowess. Though exceedingly well-planned, coordinated and executed, the comparatively low-tech means employed by the terrorists raises the possibility of a cyber strike or perhaps a more inclusive, more sophisticated assault combining both physical and virtual means on one or several critical infrastructures.

[1] The prepared statement of Mr. Cilluffo appears in the Appendix on page 83.

As we will never be able to protect everything, everywhere, all the time, from every adversary and every modality of attack, now is clearly the time for clearheaded prioritization of policies and resources. Unless we examine this issue in its totality, we may simply be displacing risk from one infrastructure to another. We need to approach the issue holistically and examine the dangers posed to our critical infrastructures from both physical attack, a well-placed bomb, and cyber attack, and perhaps most important where the two converge.

Infrastructures have long provided popular terrorist targets. Telecommunications, electric power systems, oil and gas, finance and banking, transportation, water supply systems, and emergency services have been frequent targets to terrorist attacks, and I listed a bunch in my prepared remarks. The destruction or incapacitation could have a debilitating effect on U.S. national or economic security, clearly the reason for this hearing and others.

One should state that bits and bytes or bugs and gas, for that matter, will never replace bullets and bombs as the terrorist weapon of choice. Al Qaeda, in particular, chooses vulnerable targets and varies its modus operandi accordingly. They become more lethal and more innovative with every attack. While bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse. Moreover, cyber attacks need not originate directly from Al Qaeda, but from those with sympathetic views, and given the anonymity of cyberspace, it is very difficult to discern who is really behind the clickety-clack of the keyboard.

For too long, our cyber security efforts have focused on the beep and squeak issues, and it focused on the individual virus or hacker du jour in the news, often to the neglect of the bigger picture. It is now time to identify gaps and shortfalls in our current policies, programs and procedures, begin to take significant steps forward and pave the way for the future by laying down the outlines of a solid course of action that will remedy these existing shortcomings.

Along these lines, there have already been a series of actions taken, some prior to September 11, some post. In particular, I do applaud the creation of the new cabinet-level Office of Homeland Security, directed by Governor Ridge. It is my understanding that a comprehensive review will be completed by next week, which will set out the office's roles, missions, and responsibilities. We will then have a better sense of the explicit roles and responsibilities pertaining to homeland security and how they directly impact critical infrastructure protection, and as was mentioned earlier, there was already an executive order in the works, about to be signed, on cyber security. So this is clearly something the President has been engaged in, in advancing our cyber defenses, for quite some time.

To get to the point you have brought up earlier, Mr. Chairman, this attack was a transforming event. Many have claimed that the Office of Homeland Security may not have the authority to succeed. Well, I disagree. One cannot look to history alone to identify what organizational model will be most effective. Because this is the highest priority facing our Nation today, organizational charts, titles, and line items, boxes, historic emblems of bureaucratic power, fade to the background. Governor Ridge will have the ammunition required to carry out his responsibilities because he and his mission have the full confidence of the President of the United States.

But even an undertaking of this importance takes time to move from concepts to capabilities. Once the immediacy of the problem has settled into routine, perhaps several months from now, we should consider codifying and institutionalizing its mission with congressional legislation and additional statutory authority if needed, but I think we have to crawl before we run. As both the Executive Branch and the Congress consider how best to proceed in this area, we should not be afraid to wipe the slate clean and review the matter with fresh eyes.

We need to be willing to press fundamental assumptions of national security. Critical infrastructure protection and information assurance are cross-cutting issues, but our government is still organized along vertical lines in their respective stovepipes. When we do this review, we should do it with a critical eye, not only one that appreciates how far we have to go, but also where we have come, and there have been some centers of excellence, both in government and the private sector, that we should leverage and build upon.

Ultimately, it is essential that any strategy encompasses prevention, preparedness and incident response, vis-a-vis the public and private sectors and the interface between them. What we need is a strategy that would generate synergies and result in the whole amounting to more than simply the sum of its parts, which is currently the case.

Information technology's impact on society has been profound and touches everyone, whether we examine our economy, our quality of life, or our national security. Unfortunately, our ability to network has far outpaced our ability to protect networks. Though the myth persisted that the United States had not been invaded since 1812, invasion through cyberspace has been a near-daily occurrence, a marked counterpoint to September 11 attacks.

Fortunately, however, we have yet to see the coupling of capabilities and intent, aside from foreign intelligence collection, where the really bad guys exploit the really good stuff and become technosavvy. We have not seen that marriage, but in my eyes that is a matter of time. Let me jump very briefly—I have laid out a number of recommendations that I thought we should be looking to in terms of building this partnership. As to who is responsible, it is a shared responsibility.

The government must, however, lead by example. Only by leading by example and getting its own house in order can they expect the private sector to commit the resources in both time and effort to get the job done, and we need to clarify accountability. We need to clarify roles and missions. Right now, there really is no one held accountable, and clearly that is going to be something that will be examined with all the new executive orders.

Let me skip through the rest and close with a couple of initiatives that can be taken to incentivize the private sector. First, from the government perspective, by improving the resilience of our economic infrastructure we improve the government's readiness, because so many of these critical functions are owned and operated by the private sector. But, second, we also improve our economic security, which cannot be seen as black or white. These are now blurred.

We need to encourage standards to incentivize the private sector. We need to improve information sharing, and I wholeheartedly applaud Senator Bennett's initiative in this area, because FOIA has been a significant obstacle to sharing information between the public and private sector. We can also look at liability relief. Government could provide extraordinary liability relief to the private sector in the case of cyber warfare, similar to the indemnification authority set up in the case of destruction of commercial assets during conventional warfare. So these are some of the areas we can look to.

Mr. Chairman, I know I am over my time. I have rarely had an unspoken thought. Forgive me, but not to digress, but I would like to close by saying thank you. We have all done some soul-searching in the last couple of weeks. I, for one, have never been so proud to be an American, proud of our President, proud of our Congress, and proud of the millions of Americans that make this country great. I believe we have all emerged from this with a stronger sense of purpose and appreciation of our Republic and its institutions.

This is precisely what our forefathers had in mind. We were put to the test. We will prevail. They will fail. And critical infrastructure protection is clearly an important element to improving our Nation's security.

Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Mr. Cilluffo. Wonderful, strong statement. We are proud of you, too, and all of you.

Mr. Watson.

TESTIMONY OF KENNETH C. WATSON,[1] PRESIDENT, PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY (PCIS)

Mr. WATSON. Good morning, Mr. Chairman and Senator Bennett, I am honored to be here today on behalf of the more than 70 companies and organizations from all the critical infrastructure sectors that comprise the Partnership for Critical Infrastructure Security, or the PCIS. The question: "Critical infrastructure protection: Who is in charge?" is timely, but may not have a quick and easy answer, as we have heard many times today.

We would all like to be able to turn to a single government or industry executive or agency with the authority and responsibility to assure the continued delivery of vital services to our citizens in the face of these new and emerging threats. The truth is that the infrastructure architecture requires a distributed leadership, cooperation, and partnership to accomplish that goal, exactly what Senator Bennett said earlier.

I would like to describe for you the environment of the critical infrastructures, explain what we were doing before the horrendous attacks 3 weeks ago, and what has changed since then. I will also make a few recommendations.

Over the last 10 to 20 years, the network of networks has truly changed the way we live and work. There is no turning the clock

[1] The prepared statement of Mr. Watson appears in the Appendix on page 98.

back. This has brought about unprecedented levels of productivity and profitability; however, each industry is now more dependent on every other than before, and all have come to depend on computer networks for core operations, not just as a business enhancing tool.

The Federal Government cannot function without services provided by the private sector infrastructure owners and operators. Most of these are multinational corporations with an interlaced network of suppliers, partners and customers, many of whom are outside the United States. The Internet itself relies on key name servers and routers located around the world with no central ownership or authority. Therefore, the health of the global economy is directly related to America's national and economic security.

Just as the Internet is open, borderless, international and unregulated, responsibility for protecting critical infrastructures is distributed among companies and government organizations. Form follows function. This applies not only to architecture, but also to how we organize to protect our critical infrastructures. Even with the best of intentions and the most modern tools, the Defense Department could not defend against a cyber attack on the information systems of a power plant in Omaha. That power plant must have the technologies and teams to defend itself and to prevent cascading effects beyond its own perimeter, and it must be connected to a distributed indications and warning system in order to be able to respond quickly and proactively.

Also, since every unsecured computer connected to the Internet could be used as a zombie in a distributed denial-of-service attack, these tools, teams and warnings must become part of every business' standard networking procedures. Activities that an enterprise can take: Conducting vulnerability and risk assessments; deploying security technologies; investing in research and development; resourcing and enabling incident response teams must now be distributed and coordinated.

Many in industry and government have been focusing on how to accomplish this coordination for at least the last 5 years. The President's National Security Telecommunications Advisory Committee, or NSTAC, has been providing advice on national security and emergency preparedness issues in the telecommunications sector since 1982. The NSTAC is still extremely relevant, even more today, conducting studies and holding network security information exchanges on current issues.

The President's Commission—as has been mentioned several times—on Critical Infrastructure Protection, reported in October 1997, recognizing the need for close public-private coordination, that applies to all the infrastructure sectors. Industry responded to the government's invitation to a dialogue by launching the Partnership for Critical Infrastructure Security at the World Trade Center in December 1999. Since its formation, the PCIS has become a model for cross-sector coordination and public-private cooperation.

Last year, the PCIS identified barriers to information sharing with government, and now Senator Bennett's bill and others in Congress are working through legislation based on our findings. During the response to the Code Red worm, government and industry turned to the PCIS to represent industry alongside the NIPC and security experts as we made the public service announcement that ultimately blunted the impact of that infestation. Inthe coming year, the administration will publish a public-private national plan for critical infrastructure protection, with industry sections coordinated by the PCIS.

This is not just an American problem. Several countries are establishing similar partnerships. The PCIS is forming close relationships with them and we are collaborating several areas. We are currently working with critical infrastructure protection organizations in Canada and the United Kingdom, and we are following similar activity in Switzerland. The United States and Australia conducted a bilateral meeting in August, 2 months ago, where we agreed to cooperate on security standards and in other areas.

One of the keys to success is the timely sharing of information about threats, vulnerabilities, countermeasures and best practices within and between industries and between the public and private sectors. Information Sharing Analysis Centers, or ISACs, are proving their value as both computer defense centers and awareness vehicles. There are currently five ISACs in operation: Financial services; telecommunications; information technology; electrical power; and oil and natural gas.

These ISACs have shared information on threats to members and helped their sectors prevent damage and disruption from threats like the Code Red and Nimda software worms. The telecom ISAC is able to share vital information from the government to industry that has been proved both valuable and timely. Four additional ISACs are in various stages of development: Railroads; aviation; water; and information service providers, or ISPs. One of this year's top goals for the PCIS is to establish a cross-sector and public-private information sharing architecture.

With the same goal, the existing ISACs, under the leadership of the National Communications System, met last week to work out a cross-sector operational information exchange capability. This meeting greatly accelerated the progress we have made in this area and the procedures they develop will form the foundation for the overall cross-sector architecture.

What has changed since September 11? The terrorist attacks on the World Trade Center and the Pentagon did not change the architecture of the new economy or our interdependency, or the interlinked nature of the economy's national security in the nations of the world. What those attacks did was create a sense of urgency and an increase in security awareness. Just as the administration carefully and deliberately seeks out those that conducted and supported these barbaric acts and learns about this new battlefield environment, I urge everyone involved to take the time to understand the infrastructure environment and not to move too quickly to try to solve the infrastructure protection problem.

So what can we do to protect our critical infrastructures? We need to raise the security bar worldwide, by streamlining communication and coordination, accelerating research and development, practicing good network security, and by not abandoning our values. I have four recommendations: First, support the administration initiatives to streamline coordination within the Federal Government. We will continue to work closely with the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, and the national coordinator, as the government organizes itself to manage homeland security, counterterrorism, and critical infrastructure protection.

Second, support initiatives that will secure the next generation's network of networks, as well as patches and fixes we are applying today, by providing resources to government agencies with increased responsibilities in this area and providing funding for research. To assist in this effort, the PCIS is developing a research and development roadmap that will include a gap analysis of current industry, academic and government programs, and recommendations for focusing resources to meet sector and cross-sector needs.

Third, encourage government organizations, businesses and individuals to practice sound information security, starting by adequately funding network security programs in all Federal departments and agencies; updating passwords, disallowing unauthorized accounts and unneeded services and installing firewalls and intrusion detection are no longer just common sense, but a matter of cyber civil defense.

And, last, carefully consider the impact of any new legislation on the freedoms Americans cherish: Individual privacy; freedom of expression; and freedom of entrepreneurship. We all understand that without security there is no privacy, but we must always strive for balance. My colleagues of the PCIS and I welcome any invitation to discuss our activities with you at any time. We believe a dialogue where we can hear your insight and you can hear our concerns will be healthy and fruitful.

We are all in this together: Industry, academia, the administration, the Congress, the American people, and we need all points of view to ensure that our critical infrastructures continue to meet the needs of every citizen by ensuring the continued delivery of vital services and enabling the economy that underpins our security and our way of life.

Thank you very much, and I am happy to answer any questions.

Senator CLELAND. Thank you very much, Mr. Watson. You are right. We are all in this together.

Mr. Cilluffo, I was fascinated by a comment. If you would go back in your testimony, if you could find that section where you said something about the terrorist will not do something—and ultimately will not give up bombs and bullets. Can you say that section again? Since you seemed to say that maybe bombs and bullets, in bin Laden's case, was maybe generational, and his offspring may have their finger on a mouse or something. Talk about that section again.

Mr. CILLUFFO. If we look at the threat, we need to look at a full spectrum of threats. If we are focusing on Al Qaeda specifically, this is an organization that understands the lethality, has demonstrated the capability, and bombs and bullets are the effective weapon of choice, and he will continue to accelerate the capability. If you look at it, even Al Qaeda, if you go back to Kobar Towers, you saw car bombs, then you had truck bombs at the African embassies. The *U.S.S. Cole,* you had boats as bombs. Now, unfortunately, you have planes as bombs. So it is more innovative every time, more lethal every time, he is not, and his followers in Al

Qaeda and this loosely affiliated network of radicals, because what they really do is they pool resources. There is no monolithic organization. He is the chief financial officer of this loosely affiliated organization that brings groups together.

He is not going to be turning to cyber means. They use it, cyber, for tradecraft, to communicate. Whether they use stegonography, as some media have said, I do not know, to hide code messages inside, or whether they use simple code words, where "Go walk the dog," could mean something very different, and seemingly innocuous could mean something very different if they have communications beforehand, and he has demonstrated the ability to mix very high-tech and very rudimentary low-tech means of tradecraft, to include communications.

And so I think that it is important to say that when we look at the terrorist threat today, we need to look at it holistically. We need to recognize that Al Qaeda is not all terrorism. You are going to see some that are turning to cyber means. There is only one official terrorist use of offense information warfare, and that was the Tamil Tigers of LTTE, who disabled embassy communications in Ottawa, Seoul, and Washington. But that is going to change.

What we see mostly are nations—and they are in the stealing secret business. They are not going to crash systems. They would be compromising such a valuable method and technique to steal America's secrets. So we just need to look at it holistically.

Senator CLELAND. Thank you.

Mr. Nacchio, thank you for your testimony. When I saw the Pentagon smoking and I looked at the Capitol and realized that the Capitol might be the next target, it was a strange feeling. So I tried to get on a cell phone. Of course, by now the whole system was clogged, and my immediate thought, though, was that we are also under a cyber attack. In other words, they have jammed our communications. As an old Army signal officer, I guess that was the first thing that came to my mind. Actually, I later realized the whole system was overloaded.

Also, you mentioned the reliability of the system. Again, in my training, the first week I was on active duty I had an old colonel tell me that, "Cleland, the secret to reliability is redundancy." Have you learned anything about this, in effect, instant overload, when the country is attacked or some spectacular thing happens, have you learned anything in your world that you are going to do differently? Are you going to program in more redundancy for a peak usage for a few hours, so that average citizens can communicate by the millions, which is what they wanted to do, and I just wondered if you had a comment on that?

Mr. NACCHIO. Well, yes, it is a very pertinent point, and it really relates to a question you asked an earlier panel that said how do you protect against a massive attack? The communication networks are best designed, of course, for a massive attack. There are many of them, multiple paths, physical redundancy, multiple fiber paths that you can travel. What happened in New York and the Pentagon, specifically New York, is when the towers were on fire, West Street central office of Verizon went out, so all of southern Manhattan, at the end point, was taken out. The rest of the nationwide infrastructure worked well, but you could not get in and out of southern New York, and similarly the wireless networks and points did not work if you were going in and out of New York or in and out of northern Virginia.

But the rest of the Nation, communicating about it, worked well. So you still have physical points of vulnerability. What we learned here is that what we used to protect for a nuclear attack, the same thing could happen with an airplane attack or if we had a massive fiber cut or if a bridge across the Mississippi River went down. These infrastructures need to be protected. So we are not invulnerable to physical attacks, and that is what was demonstrated, but it is very isolated.

The bigger danger is what my colleague here on the left has said; it is only a question of time, only a question of time that what nation-states can do to attack the fiber infrastructure, terrorists will learn how to do, and you will see a massive shutdown, and that is what I know national security has worried about in the past and what we have tried to assist on, a massive cyber attack that disables nationwide communications, not just a pair of points, say in New York or Washington.

Senator CLELAND. Then do we in the Federal Government and many in the private sector need to think about redundancy, some kind of redundant capability?

Mr. NACCHIO. Right.

Senator CLELAND. Certain leaders were moved to, in effect, a redundant headquarters outside of Washington. In the case of, shall we say, a national emergency in our telecommunications world, in our cyber world, do we need to be able to have some kind of built-in redundancy?

Mr. NACCHIO. Absolutely, and I think for most of the infrastructure in this country, you have redundancy. There are still critical points and there is a limit at the last mile, so to speak, at some point you are not going to have redundancy, and that is what we have to be careful of.

Senator CLELAND. Thank you.

Mr. Watson, do you have any feeling about your own view about whether an Office of Homeland Defense is going to be adequate, or do you feel a cabinet-level agency with budget and with troops in the field and so forth, massing their assets, is something we ought to seriously think about? Have you come to a conclusion on that?

Mr. WATSON. There are many agencies and organizations in the Federal Government that are currently contributing to the critical infrastructure protection effort. There certainly needs to be some streamlining. I am in no position to tell the government how to organize itself, but simply the fact that the pending executive order seems to indicate that there will be someone to coordinate critical infrastructure protection, we believe, is a very positive step, and we look at that as a parallel effort to what we have at the PCIS, coordinating all the infrastructure sectors.

Senator CLELAND. Mr. Cilluffo, I see your head nodding. Do you want to come in on that?

Mr. CILLUFFO. Oh, no, I pretty much agree. What we will have to work out are the details, of course. There are a number of potential executive orders out there, a number of great ideas and a number of commissions that have come out with different ideas. What

I think you are seeing now is the amalgamation of the best of the best. There is no right answer. Whatever answer they choose, though, is in some ways the right answers, because they are the ones who are going to have to implement and execute.

So what I say here is let's not rush to judgment. Let's see where this goes. Six months from now, maybe we are going to see there is a need for additional statutory authority or very specific legislative proposals or even access to troops. But I think let's focus now on the short-term needs requirements, backfill those threats to be able to withstand, prevent and preempt an incident, make sure that we are looking at this from not just the top-down, but the bottom-up; that our emergency responders and the public health community, for a bio event, are ready. So I do not disagree, but I think now let's focus on the short-term and then look to long-term capacity building.

Senator CLELAND. Ms. Gorelick, any ideas?

Ms. GORELICK. As I said earlier, I think we do need some streamlining from the point of view of business to know who is doing what, operationally. I would make a comment about NSTAC in that regard. The reason that NSTAC is as robust as it is and has the capacity that it does, compared to the other ISACs that are more nascent, is that it was actually stood up by the government. The CEOs of the industry were, in 1982, named to the panel. They were given clearances. They get briefings. There is an extant staff. Industry is not told what to do by the government, but there is an infrastructure provided.

There are many willing partners in the private sector, and we have a lot of technical expertise. We understand, from our own business perspective, the need to have business continuity. We understand, from our own business perspective, the need for our partners to have business continuity, but we are in business, we are unused to collective or collaborative action of the sort that is really called for here. If you could have the NSTAC model in each of the other industries, you would have a much more robust capacity on the part of industry doing the sorts of things that Mr. Watson is talking about. Other industries would get caught up to where communications is.

The financial services sector did very well, considering what happened to it. It does have a lot of individual redundancy. We have backup centers and we have done a lot of thinking about hardening those resources. But if we are going to get where we need to be as industries responsible for this national infrastructure, I think we need, as I suggest in my written testimony, more adequate support on an industry by industry basis. I think we would be all helped by that. I do not think it is tremendously expensive, and it would dramatically increase the way that industry and government communicate with each other, and that industry communicates across itself.

Senator CLELAND. Mr. Nacchio.

Mr. NACCHIO. Mr. Chairman, let me just build on that—a couple of quick thoughts. Something that we do in the private sector, I think, applies here. If you want to get something done, define it clearly, focus and align resources, and keep it simple. Today, when we have a problem on our networks, we are required under the law to report it within 30 minutes to the FCC, as Verizon did to Chairman Powell when they had the outage. If we, NSTAC members, are faced with a cyber attack, will report it to NSTAC so it can be shared. But just to be clear, we take care of ourselves. NSTAC does not direct what we do. We are together.

I have a fiduciary responsibility to make sure my network does not go down no matter who is attacking. I have my own guys who protect it. We hire ex-FBI, ex-anybody we can. We are kind of a nation-state in defending our physical and our cyber infrastructure. We are happy to share that as long—under the Freedom of Information Act—as it not get passed out to the bad guys, so to speak.

So what NSTAC is really good at, which I think was touched here and why I am involved, is that my biggest job as the vice-chair is not necessarily working with national security, it is working with all my colleagues in industry as best I can to encourage them, based upon what we learned, because we are all responsible for this, not just the government. But if you can keep it focused and keep it simple, your pertinent question about what do you do about homeland defense—I could not tell you how to organize the government—but I would say keep it simple.

There are at least a dozen agencies, if something really bad is happening, we have to call, and that is all good, including the FBI, the local police, and the FCC. We generally get on it ourselves to start with. So, I recommend that you can keep it focused, streamlined, with clear accountability, and, of course, dedicate the resources.

Ms. GORELICK. I would second that.

Senator CLELAND. Thank you. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman.

Mr. Nacchio, they taught me in high school that nature abhors a vacuum. Government abhors simplicity. [Laughter.]

Senator BENNETT. And may I, as a former customer of US West, and now one who writes a check to you every month, thank you for the improvement in service that has come since you took over. We are grateful that you have put the kind of resources you have into increasing customer service, and it is not unnoticed and not unappreciated.

Mr. NACCHIO. Thank you.

Senator BENNETT. Mr. Nacchio has told us what they did at September 11. I would be interested, Ms. Gorelick, what Fannie Mae did with respect to September 11.

Ms. GORELICK. We stayed in business.

Senator BENNETT. What kind of challenges did you face?

Ms. GORELICK. We were open for business. Our challenges were communication with sources of funding. The capital markets, as you know, were not really operating. We were able to establish communication with the Fed. We were able to maintain our communications with our customers.

Basically, what we do, as you know, is fund those who are making mortgage loans around the country, and, by and large, the other outlets were, at least for the period of September 11 and for some period after that, not able to function. Fortunately, for us, we were able to. We have a very robust system. Like Mr. Nacchio, we try to hire the best. Our head of security is out of DISA. We have spent a lot of time thinking about cyber security.

So we were able to function and I think we were able to perform a real service to those who needed the capital markets to function. Eventually, those markets came back, but it took awhile, and I think if you look at what some of the learnings are, I think a lot of financial services companies have learned what makes their backup systems work. If you have your backup system right down the street from your main system, that may not work. If your backup system is reliant on the same communications grid, even if it may be in Brooklyn rather than lower Manhattan, it may not work.

If you have a backup system that relies on the same people and the people cannot get there, it may not work. Fannie Mae did not experience any of those problems, and that is partly good planning and partly good luck, but I think there are a lot of learnings for the financial services sector coming out of this event.

Senator BENNETT. Thank you.

Mr. Cilluffo, you made reference to the motivations of Al Qaeda, and I will share with you and put into this record information that came from a hearing we held in the Joint Economic Committee on this issue less than 60 days ago, where I asked one of the witnesses from the CIA if, in fact, the next terrorist attack would not come in the form of a cyber attack, because I said, as I said before, if I were someone who wished this country ill—back to your world, Ms. Gorelick—I would want to shut down the Fed wire and break into the computer system that keeps that going. If you could do that, you would produce long-term devastation.

Ms. GORELICK. If I might suggest, Senator Bennett—I am sorry to interrupt—but I would actually think it useful to inquire as to what occurred, because that is a very vulnerable node, and we saw——

Senator BENNETT. We have done that on the Banking Committee. I sit on the Banking Committee, and I have asked Alan Greenspan directly about that issue and have had my staff down at the Fed looking at it for exactly the reason that you are underscoring. The answer I got from the witness was very interesting, and, in view of what has now happened, prophetic. He said, "Senator, that is because you think the way you think. To the terrorist, shutting down the Fed wire does not give him what he wants, which is television footage that can be broadcast around the world to inflame people," and one of the analysts after September 11 who spoke to us said, "In a sense, this attack by Al Qaeda backfired and failed, because what they wanted to produce was such a reaction out of America as to create a war of civilizations that would then polarize the Muslim world on their side. It backfired in that it caused such revulsion among good Muslims, who said this is not what they teach in the Koran, that it has driven moderate Arab States and Muslim States to our side in this confrontation." So cutting down the Fed wire does not give them any footage at all on international television, and therefore was not a notion that he looked at.

But we go to the issue of hostile nation-states, and the ability to shut down the Fed wire would be something that a dictator in a hostile nation-state could hold this country hostage, a phone call or a hotline to the President of the United States, saying, "Mr. President, we want the following things done in the international scene, and if they are not, within 20 minutes," or they would probably give him less time than that, "the Fed wire will be shut down and the American economy will come to a screeching halt."

If we think in strategic terms, isn't that the kind of long-term protection that we have got to deal with, in addition to the immediate challenge of terrorists that want to use kinetic weapons—isn't this the long-term strategic vulnerability that we have?

Mr. CILLUFFO. Absolutely, Mr. Chairman—Senator Bennett.

Senator BENNETT. I will take that, but the Senate probably would not concur. [Laughter.]

Mr. CILLUFFO. But let me build on what I thought was such an important point. The single common denominator of all terrorism is that it is a psychological weapon intended to erode trust and undermine confidence in a government, its institutions, its elected officials, its policies in a region or, more generally, its values, and on and on and on and on. This did backfire. It united our country and it united—we united at home and we built a united front abroad. In the back of the minds, I think, of the administration, they have done a wonderful job of keeping this to fighting the really radical radicals. This is not about Islam. It is about radical Islamic fundamentalism, which Islam abhors, and we need to keep it that way.

But, to the cyber question, I do not think there is an easy answer. Since the end of the Cold War, threat forecasting has arguably made astrology look respectable, and I do not have a crystal ball, but I would say that one thing we do want to think about in terms of conventional terrorist organizations are combined attacks, where perhaps you detonate your conventional explosive, big, large, whatever it may be, and you disrupt emergency 911, so the first responders cannot get to the scene, or something similar—and we do not want to advertise too many possibilities.

But you are right. In terms of nations, that is where we have seen capabilities. There is no question that nations are doing surveillance, the cyber equivalence of intelligence preparation of the battlefield, on our networks. And those same tools to steal secrets can automatically be turned on to deny service, to attack. So this is something we need to be looking at, absolutely, and we need to be looking at it in a many-pronged lens. We need to improve our own computer network, exploit the ability to steal cyber secrets of others, as well as good old espionage.

Senator BENNETT. If I could just make one quick comment, Mr. Chairman, before we wind it up. One of the vulnerabilities that we have to deal with, with the Defense Department, is the potential ability of an enemy to break into that communications system and then send the wrong instructions to the CINCs, and even if they do not, the mere fact that there is the possibility that they have will cause the CINC not to act on real instructions until he can be absolutely sure, through redundancy, that this order did come from the CINC, and in that process, time is lost, efficiency is lost, and the combination that Mr. Cilluffo was talking about of a kinetic weapon attack and then a scrambling of our command and control system or a threatening of our command and control system that slows down our response is an additional tool of warfare that we need to deal with as we are thinking about this in strategic long-term——

Mr. WATSON. Senator Bennett, if I may make an additional comment to piggyback on that, I spent 23 years in the Marine Corps, the last eight of which were devoted to what became information warfare, and we were very much concerned with the combination of things like electronic warfare, military deception, psychological operations, destructive capabilities. But our feeling now in the private sector—and there are many of us that believe that the center of gravity for this country has moved to the private sector, because everyone is dependent on the private sector for the services that the infrastructures provide, we understand that we are on the front lines of defense, and I think it is impressive that the board of directors of the PCIS is all volunteer, and they all represent presidents and executives from companies like Bank of America, BellSouth, Consolidated Edison, Union Pacific, Conaco, Microsoft, and Merrill Lynch. You name the industry association and they are on the board. We get it, and we are ready to cooperate and help.

Senator BENNETT. Thank you. Thank you, Mr. Chairman.

Senator CLELAND. Thank you, Senator Bennett, and thank our panelists today, wonderful testimony.

In conclusion, talking about the unity that has been brought about here, I have been often asked about the historical impact of the attack on September 11, and I quote Admiral Yamamoto, who planned and executed the attack on Pearl Harbor, that afterwards he felt he had only awakened a sleeping giant, and in so many ways that is exactly what has happened.

Thank you all very much. The hearing is adjourned.

[Whereupon, at 11:59 a.m., the Committee was adjourned.]

APPENDIX

PREPARED STATEMENT OF SENATOR BUNNING

Thank you, Mr. Chairman.

This is the second hearing on critical infrastructure protection the Committee has held this year, and I am pleased we are looking at this issue again.

The first hearing the Committee held was on September 12, the day after the terrorist bombing. The importance of our security has never been more evident, as the reality of terrorism on America's soil was sadly brought home.

Protecting critical infrastructure is a responsibility of all levels of government and the private sector.

This will require businesses and government to share information and form alliances in ways they have traditionally not done.

I am hopeful that we can make some good progress in protecting our critical infrastructure from future attacks over the next couple of months.

However, we have a long way to go.

In fact, during the September 12 hearing we discussed that too often in the Federal Government our critical infrastructure is weakened because simple, commonsense steps are not taken.

This includes not changing passwords routinely or closing accounts for former employees or contractors.

This leaves us vulnerable to future attacks. We must do better.

I want to thank our witnesses for being here today, and look forward to hearing more about what else we need to do to protect our critical infrastructure.

"CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE?"
COMMITTEE ON GOVERNMENTAL AFFAIRS
THURSDAY, OCTOBER 4, 2001
9:30 a.m. Room 342
DIRKSEN SENATE OFFICE BUILDING

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, members of the Committee on Governmental Affairs, it is an honor to appear before you today to discuss the Federal government's ongoing efforts to help secure our nation's critical infrastructures. Earlier efforts are described in some detail in the *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001.*

The Committee on Governmental Affairs has shown exceptional leadership on a broad range of national and economic security issues. This is particularly true in regard to Critical Infrastructure Assurance. I am therefore grateful for the opportunity to work closely with you and the Congress to develop ways to advance infrastructure assurance for the private sector, for the federal, state and local governments, and in fact, for all Americans.

As you know, President Bush has declared that securing our critical infrastructures is essential to our economic and national security and will be a priority of his administration. The tragic events of September 11th only underscore the urgency with which we must undertake this vital task as one component of a broader effort to secure the nation's homeland against terrorism.

No viable solutions – especially on a matter of such complexity and scope - can be developed or implemented without the executive and legislative branches working closely together, and in the coordinated, complimentary manner that they are.

As vital as our nation's critical infrastructures are to the American Way of Life, the authority to protect those infrastructures must be a priority; and the resources must match the rhetoric. I am excited by the Common Purpose that has joined the Executive and Legislative branches of our great government in implementing an Agenda for Action.

The work of your committee, along with that of others, will make an important contribution to establishing the consensus and leadership focus needed to safeguard critical government and private sector services against both physical and cyber attacks. As we have so recently seen, the enemy is ruthlessly attacking economic targets – our critical infrastructures – in a misguided effort to bend our wills and undermine our resolve.

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 of 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 – we are painfully witnessing this now - could have a debilitating regional or national impact. These infrastructures relate to:

- Information and communications,
- Electric power generation, transmission, and distribution,
- Oil and gas production and distribution,
- Banking and finance,
- Transportation,
- Water supply, and
- Emergency government services.

Critical infrastructure assurance is concerned with the readiness, reliability, and continuity of infrastructure services 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 THE CRITICAL INFRASTRUCTURE COMPONENTS

Threats to critical infrastructure fall into two general categories:

- Physical attacks against the "real property" components of the infrastructures; and

- Cyber attacks against the information or communications components that control these infrastructures.

Infrastructure owners and operators have always had primary responsibility for protecting their physical assets against unauthorized intruders. Yet these measures, however effective they might otherwise be, were generally not designed to cope with significant military or terrorist threats. Nor -- until recently -- did they have to be. The Defense Department, Justice Department, and other Federal agencies have contributed significantly to the physical protection of the nation's critical infrastructures through the defense of our national airspace and borders against attacks from abroad. Clearly the events of September 11th are going to require both government and industry to work together to deal with the new challenges of terrorism against our homeland.

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. The vast majority of the nation's infrastructures are privately owned and operated -- government action alone cannot secure them. Only an unprecedented partnership between private industry and government will work.

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. Individuals and groups seeking to exploit these vulnerabilities range from the recreational hacker to the terrorist to the nation state intent on obtaining strategic advantage.

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?

FEDERAL ENTITIES INVOLVED IN INFRASTRUCTURE PROTECTION

Taking the broad view, it would be accurate to say that each Department and Agency in the Federal government contributes to the objective of critical infrastructure assurance. The heads of executive departments and agencies are responsible and accountable for providing and maintaining appropriate levels of information systems security, emergency preparedness, continuity of operations, and continuity of government for programs under their control.

Under Presidential Directive 63, the previous administration assigned overall responsibility for policy development and coordination for critical infrastructure assurance to the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council.

PDD-63 established the National Infrastructure Protection Center (NIPC) housed at the FBI. NIPC serves as the nation's threat assessment, warning, and incident response center for cyber attacks, and also facilitates law enforcement investigations of cyber-related crimes.

PDD-63 also established the Critical Infrastructure Assurance Office (known as CIAO) as an interagency office located at the Department of Commerce to support the National Coordinator in carrying out these policy development and coordination functions.

CIAO's responsibilities in developing and coordinating national critical infrastructure policy focus on three key areas:

- Promoting national outreach and awareness campaigns both in the private sector and at the state and local government level;
- Assisting Federal agency analyses of critical infrastructure dependencies; and
- Coordinating the preparation of an integrated national strategy for critical infrastructure assurance.

I want to share with you my views on what must be done and what we have done.

Promote National Awareness

Our first responsibility is to raise national awareness about the problem of critical infrastructure assurance. The primary focus of these efforts has been on the critical infrastructure industries. The target audience has been the corporate boards and chief executive officers who are responsible for setting company policy and allocating company resources. The basic message has been that critical infrastructure assurance is a matter of corporate governance and risk management. Senior management must understand that they are responsible for securing corporate assets -- including information and information systems. Corporate boards must understand that they are accountable, as part of their fiduciary duties, to provide effective oversight of the development and implementation of appropriate infrastructure security policies and best practices.

Prior to September 11th, the challenge of our national awareness effort was to present a compelling business case for corporate action. Government concerns about economic and national security, while important, were not generally viewed as sufficiently providing such a case. Threats of "cyber terrorism" and "information warfare," while legitimate, were not readily executable in the market – they appeared too remote and irrelevant to a company's bottom-line. That has all now changed.

The threats to critical infrastructure are being translated into business impact that corporate boards and senior management understand. Business impact includes operational survivability, shareholder value, customer relations, and public confidence. Corporate leaders are beginning to understand that the tools capable of disrupting their operations are readily available, and are not the monopoly of nation states. The risks to their companies are serious and immediate and, thus, require prompt attention.

In addition to infrastructure owners and operators, awareness efforts have also targeted 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.

Once the private sector acknowledges the problem of critical infrastructure assurance as one that it must solve through corporate governance and risk management, our role has been to facilitate corporate action.

The government should encourage appropriate information sharing within and among the infrastructure sectors and between the sectors and government. The information shared could include system vulnerabilities, cyber incidents, trend analyses, and best practices. The reason companies should be encouraged to share this kind of information is because by doing so they will obtain a more accurate and complete picture of their operational risks, as well as acquire the techniques and tools for managing those risks.

The Federal government also should encourage the infrastructure sectors to work together on developing contingency plans for coordinating their responses in the event of major service disruptions, whatever the precipitating cause. As the infrastructures become more interdependent, there is a growing risk that restoration efforts undertaken by one sector could adversely affect the operations or restoration efforts of another, potentially contributing to further service disruptions.

In addition, the government should work with industry in identifying potential legal and regulatory obstacles that may unduly impede information sharing or might otherwise interfere with voluntary efforts by the business community to maximize information security efforts. For example, some in industry have argued that voluntary information sharing cannot proceed to a fully mature corporate activity until the reach and impact of laws governing anti-trust and tort liability and the Freedom of Information Act are clarified.

CIAO promotes activities that inform business and technology leaders across industry sectors of the need to manage the risks that accompany the benefits associated with reliance on information systems. CIAO focuses on initiatives that cut across industry sectors and are not the existing responsibility of agencies.

CIAO's outreach activities are reflected in the following major initiatives:

- The Partnership for Critical Infrastructure Security; and

- Outreach to the business risk management community;

Partnership for Critical Infrastructure Security: As individual Federal agencies formed partnerships with each critical infrastructure sector, there emerged a need for cross-industry dialogue and sharing of experience to improve effectiveness and efficiency of individual sector assurance efforts.

The Partnership for Critical Infrastructure Security was convened in response to that expressed need. This partnership of over 70 companies provides a unique forum for government and private sector owners and operators of critical infrastructures to address issues of mutual interest and concern.

The Partnership also engages other stakeholders in critical infrastructure protection, including the risk management (audit and insurance), investment, and mainstream business communities. The Partnership, which builds upon public-private efforts already underway by the Federal Lead Agencies, is organized by industry for industry, with the U.S. Government acting as a catalyst and a participant.

Major topics being addressed by the Partnership include: approaches to assessing interdependency vulnerabilities; multi-sector information sharing; legislative and public policy issues; research and workforce development; industry participation in preparing the emerging version of the national strategy; and outreach to state and local governments.

Business Risk Management Community: The business risk management community, consisting of auditors, financial security analysts, the insurance community, the legal community, and financial reporting boards serve as unique channels of communication to senior leadership of industry. These groups work with industry in assessing business risks, communicating noteworthy changes to those risks, and supporting the management of such risks.

In that regard, CIAO implemented an awareness and education partnership with a consortium consisting of the Institute of Internal Auditors, the National Association of Corporate Directors, the American Institute of Certified Public Accountants and the Information Security Audit and Control Association. This consortium brought the involvement of a number of noted insurance firms, risk management professionals, legal counsel, corporate board members, audit experts, and Wall Street security analysts.

The consortium held a series of five regional conferences, called "Audit Summits." These meetings were hosted or sponsored by prominent companies, such as J.C. Penney, Home Depot, New York Life Insurance, Oracle Corporation, Arthur Anderson, Deloitte & Touché Tohmatsu, PriceWaterHouseCoopers, and KPMG. The target audiences were directors of corporate boards, chief auditors, and other corporate senior executives. The meetings produced a report that provided guidance for corporate boards on managing information security risks.

Federal Infrastructure Dependencies

The Federal government is responsible for performing certain functions and delivering certain services essential to "providing for the common defense," "promoting the general welfare," and "insuring domestic tranquility."

Such functions and services are vital to advancing our national security, foreign affairs, economic prosperity and security, social health and welfare, and public law and order. Examples from the pages of our nations' newspapers include:

- The mobilization of our Reserve Forces –

- The protection of the U.S. homeland -

- The projection of U.S. forces overseas –

- The ability to maintain critical government communications during crises involving national security or a national emergency –

- Timely warnings of potential terrorist or cyber-activist attack –

- And even something as basic but yet important to a significant segment of the population as the delivery of social security checks.

Increasingly, these services depend ultimately on privately owned and operated infrastructures. To advance this vital Federal interest, the government must take a leading role and satisfy a number of requirements.

Each Federal department and agency must identify:

- Its essential functions and services and the critical assets responsible for their performance;

- All associated dependencies on assets located in other departments and agencies that are necessary to performance or delivery; and

- All associated dependencies on privately owned and operated critical infrastructures that also are essential to performance or delivery of services.

The CIAO's Project Matrix was developed to assist civilian Federal agencies in this process.

To illustrate, I will use the example of the Commerce Department's Tropical Prediction Center (the "TPC") in Miami, Florida, which is responsible for providing timely warnings of hurricanes.

Incapacity or destruction of this essential government service could result in considerable loss of life and property. Indeed, thousands of people died during the Galveston, Texas hurricane of 1900 because there was no advance warning of the hurricane's approach and, thus, no one evacuated the city. In 1992, Hurricane Andrew would have been even more devastating than it was had the TPC not been able to provide timely information about the storm, thereby enabling thousands to evacuate from those areas where the storm's predicted strength threatened to be greatest.

Although the TPC is a critical asset, it does not operate in isolation; it depends on a variety of other government agency assets, as well as assets owned and operated by private government contractors. These include satellite imaging and analysis centers and radio transmission facilities located in Maryland and Pennsylvania.

Operational disruptions at any one of these facilities could impede the delivery of timely hurricane warnings just as effectively as operational disruptions at the TPC itself.

Furthermore, the TPC depends on specific providers of critical infrastructure services to operate, including Florida Power & Light for electric power, and Bell South & MC 2000 for telecommunications. Disruptions to these services also could impede TPC operations that are necessary to deliver hurricane warnings.

Once such critical assets and associated dependencies are identified, Federal departments and agencies must assess their vulnerability to physical or cyber attack. If they are determined to be vulnerable, departments and agencies must develop and implement plans to manage the risks posed by potential attacks to the performance of essential functions and services.

These plans should seek to deter attacks from happening in the first place, protect critical assets from damage or destruction if attacks occur, mitigate the operational impact of attacks if protective measures fail, restore operations if attacks disrupt services, and reconstitute assets if damaged or destroyed during attacks.

Where performance of essential government functions and services depends on privately owned and operated infrastructures, Federal departments and agencies must work with the owners and operators of these specific infrastructure companies -- on mutually agreed upon terms -- to ensure adequate security measures are established and maintained.

Development of a National Strategy

A common vehicle of communicating overall critical infrastructure policy and strategy is essential. A national strategy developed jointly between government and industry is an effective means for arriving at an agreement about respective roles and responsibilities. The purpose of such a strategy is to present an integrated public-private strategy for government and industry to chart a common course toward achieving the overall goal of national critical infrastructure assurance. CIAO is currently in the process of preparing a national strategy – in coordination with other Federal departments and agencies and the private sector.

The resulting document will serve not only as a guide for action, but also as a vehicle for creating consensus in Congress and with the American people on how to proceed. A national strategy will also help to establish the basis with the Congress and the American public for proposing legislative and public policy reforms where such reforms are needed to advance national policy.

The development of a national strategy should not be viewed as an end in itself. It should be part of a dynamic process in which government and industry continue to modify and refine their efforts at critical infrastructure assurance, adjust to new circumstances, and refine the national strategy as appropriate.

CLOSING REMARKS

Thank you for the opportunity to share my views with you this morning. I look forward to continuing our dialogue.

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

October 4, 2001

Mr. Chairman, Ranking Member Thompson, and members of the committee, thank you for inviting me here today to testify on the topic, "Critical Infrastructure Protection: Who's in Charge?" Holding this hearing demonstrates your individual commitment to improving the security of our critical infrastructures and this committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. The September 11 attacks on the World Trade Center and Pentagon have demonstrated how a significant disruption to the transportation industry or any other critical infrastructure will certainly have a ripple effect on others. My testimony today will address our role in protecting the Nation's infrastructures and how we coordinate with other entities.

As set forth in Presidential Decision Directive 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." The NIPC is the only organization in the federal government with such a comprehensive national infrastructure protection mission. The NIPC gathers together under one roof representatives from, among others, the law enforcement, intelligence, and defense communities, who collectively provide a unique analytical perspective to threat and incident information obtained from investigation, intelligence collection, foreign liaison, and private sector cooperation. This perspective ensures that no single "community" addresses threats to critical infrastructures in a vacuum; rather, all information is examined for its potential for simultaneous application to security, defense, counterintelligence, terrorist or law enforcement matter.

While developing our infrastructure protection capabilities, the NIPC has held firm to two basic tenets that grew from extensive study by the President's Commission on Critical Infrastructure Protection. First, the government can only respond effectively to threats by focusing on protecting assets against attack while simultaneously identifying and responding to those who nonetheless would attempt or succeed in launching those attacks. And second, the government can only help protect this nation's most critical infrastructures by building and promoting a coalition of trust, one . . . amongst all government agencies, two . . . between the government and the private sector, three . . . amongst the different business interests within the private sector itself, and four . . . in concert with the greater international community. Therefore, the NIPC has focused on developing its capacity to warn, to investigate, and to build partnerships, all at the same time. As our techniques continue to mature and our trusted partnerships gel, we will continue to witness ever-better results.

Over the past three years, we cultivated a number of initiatives that have developed into increased capabilities, all of which are being actively used to mitigate the terrorist threat and to prepare our response to the events of September 11th. The NIPC has developed InfraGard into the largest government/private sector joint partnership for infrastructure protection in the world. We have taken it from its humble roots of a few dozen members in just two states to its current membership of over 2,000 partners. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service we provide to InfraGard members free of charge. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and other critical infrastructure vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices and several of its Resident Agencies (subdivisions of the larger field offices).

A key element of the InfraGard initiative is the confidentiality of reporting by members. The reporting entities edit out the identifying information about themselves on the notices that are sent to other members of the InfraGard network. This process is called sanitization and it protects the information provided by the victim of a cyber attack. Much of the information provided by the private sector is proprietary and is treated as such. InfraGard provides its membership the capability to write an encrypted sanitized report for dissemination to other members. This measure helps to build a trusted relationship with the private sector and at the same time encourages other private sector companies to report cyber attacks to law enforcement.

InfraGard held its first national congress from June 12-14, 2001. This conclave provided an excellent forum for NIPC supervisors and InfraGard members to exchange ideas. InfraGard's success is directly related to private industry's involvement in protecting its critical systems, since private industry owns almost all of the infrastructures. The dedicated work of the NIPC and the InfraGard members is paying off. InfraGard has already prevented cyber attacks by discreetly alerting InfraGard members to compromises on their systems. On May 3, 2001, the InfraGard initiative received the 2001 WorldSafe Internet Safety Award from the Safe America Foundation.

The NIPC also reaches out to the entire public with its website at nipc.gov, which to date has provided systems administrators and home users alike with significant warnings about cyber threats and vulnerabilities. As recently as last week, we provided information systems security advice through our website, InfraGard, and our other partnerships, to better protect the public from the Nimda worm. In fact, based on our prior responsiveness to the Code Red worm and our joint efforts with the private sector in publicizing preventive measures that business and home users could put in place, we believe the impact of the Nimda worm, which took advantage of similar software vulnerabilities as Code Red, was significantly reduced.

Our website provides the public with the ability to report computer attacks and intrusions online, simply by filling out and submitting an Incident Reporting Form. The NIPC also provides timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure best practices through its bi-weekly publication *Cybernotes*. The NIPC provides policy and decision-makers information about current events, incidents, developments and trends related to critical infrastructure protection through its monthly publication called *Highlights* and, more significantly, by bringing groups together to meet on important issues. We have established these and other mechanisms to promote meaningful two-way communication with the public, and they are seeing active use.

The NIPC's Watch Center operates around the clock and communicates daily with the Department of Defense and its Joint Task Force for Computer Network Operations (JTF-CNO). The Watch Center is also connected to the Watch Centers of several of our close allies. U.S. Army Major General Dave Bryan, Commander of the JTF-CNO, recently remarked that, "The NIPC and JTF-CNO have established an outstanding working relationship. We have become interdependent, with each realizing that neither can totally achieve its mission without the other." I couldn't agree more. The NIPC's ability to fulfill the expectations and needs of its Department of Defense component is achieved by the inter-agency structure of the Center, which includes the NIPC's Deputy Director Rear Admiral James Plehal, USNR, and the NIPC's Executive Director, Steven Kaplan, a Supervisory Special Agent from the Air Force Office of Special Investigations. The Section and Unit Chiefs in the Computer Investigation and Operations Section and the Training, Outreach, and Strategy Section are from the FBI. The Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service, and the Unit Chief of ISAC Support and Development is a senior CIA analyst. The Section Chief of the Analysis and Warning Section is from the CIA and his deputy is a senior FBI agent. The head of the NIPC Watch and Warning Unit is reserved for a uniformed service officer, and the head of the Analysis and Information Sharing Unit is staffed by a National Security Agency manager. The Center's staffing demonstrates our desire for broad, high-level, multi-agency ownership of the NIPC and our collective commitment to achieve meaningful and effective coordination across the law enforcement, intelligence, defense, and other critical government operations communities.

Within the Center, the NIPC has full-time representatives from a dozen federal government agencies, led in number by the FBI and the Department of Defense, as well as from three foreign partners: the United Kingdom, Canada, and Australia. We are also strong partners with the General Services Administration's Federal Computer Incident Response Center, FedCIRC, in order to further secure our government technology systems and services. We also team up regularly with the CIA and NSA to work on matters of common concern. In addition to interagency participation, the NIPC has established information sharing connectivity with a number of foreign cyber watch centers, including in the UK, Canada, Australia, New Zealand, and Sweden. And, we continue to take advantage of the FBI's global presence through its Legal Attache offices in 44 nations.

Our multi-agency team works with Information Sharing and Analysis Centers (ISAC's) throughout the country, including those that represent the Financial Services Sector, the Electric Power Sector, the Telecommunications Sector, and the Information Technology industry. In addition to these private sector partners, we have provided threat briefings to the Water, Oil and Gas, Financial, Electrical Energy, Information Technology, Telecommunications, and Railroad Sectors. Since September 11th, the NIPC has been providing sector briefings almost every day. We are also connected with the 18,000 police departments and Sheriff's offices which bravely serve our nation daily and in times of crisis. This past March the NIPC and the Emergency Law Enforcement Services Sector Forum completed the nation's Emergency Law Enforcement Sector Plan together with a "Guide for State and Local Law Enforcement Agencies." This significant achievement represents the nation's first and only completed sector plan and it is being used as a model by the other critical infrastructure sectors. Taken together, the Plan and the Guide provide our emergency law enforcement first responders with procedures that are immediately useful to enhance the security of their data and communications systems.

While the NIPC works diligently with its interagency and private sector partners, it has embraced other initiatives and fulfilled its role in leading the critical infrastructure protection effort. This is evidenced by its coordinating actions as Chair of the Incident Response Sub-Group of the Information Infrastructure Protection and Assurance Group established by National Security Policy Directive-1. The NIPC also routinely disseminates information through its participation in task forces and working groups that meet regularly. NIPC senior leadership participates in weekly senior level meetings to exchange strategic level information with the Assistant Secretary of Defense for Command, Control, Communication and Intelligence. Further collaboration is demonstrated through the NIPC's designation as chair of one of the subcommittees that is revising the National Plan.

While the NIPC has made great strides over the last three years, we recognize the need to do better, and we are working diligently to improve. In a GAO report dated April 25, 2001, the NIPC was recognized as having an effective investigative training and InfraGard program. In his prepared statement for the May 22, 2001 hearing, GAO's Director of Information Security, Mr. Robert F. Dacey, stated:

> First, the NIPC has provided valuable coordination and technical support to FBI field offices, which have established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC has supported these investigative efforts by (1) coordinating

investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for the NIPC field squads and teams.

Over the past three years, NIPC has provided training for more than 2,500 participants from federal, state, local and foreign law enforcement and security agencies. The NIPC's training program complements training offered by the FBI's Training Division as well as training offered by the Department of Defense and the National Cybercrime Training Partnership. Trained investigators are essential to our successfully combating computer intrusions.

Enhancing Capacity for Strategic Analysis

The GAO recognized that the NIPC's ability to completely achieve its mission was most affected by a shortfall of personnel resources. Specific recommendations included enhancing capacity for strategic analysis. I am pleased to report progress in this area.

We have established four strategic directions for our capability growth through 2005: prediction, prevention, detection, and mitigation. None of these are new concepts but NIPC has renewed its focus on each of them in order to strengthen our strategic analysis capabilities. NIPC has worked to further strengthen its longstanding efforts on the early detection and mitigation of cyber attacks. These strategic directions will be significantly advanced by our intensified cooperation with federal agencies and the private sector. As the recent Leaves, Code Red and Nimda worm incidents demonstrate, our working relations with key federal agencies, like FedCIRC, NSA, CIA, and the Joint Task Force - Computer Network Operations (JTF-CNO), and private sector groups such as SANS, the anti-virus community, and the major Internet service providers and backbone companies have never been closer. Our most ambitious strategic directions, prediction and prevention, are intended to forestall attacks before they occur. We are seeking ways to forecast or predict hostile capabilities in much the same way that the military forecasts weapons threats. The goal here is to forecast these threats with sufficient warning to prevent them. A key to success in these areas will be strengthened cooperation with intelligence collectors and the application of sophisticated new analytic tools to better learn from day-to-day trends. The strategy of prevention is reminiscent of traditional community policing programs but with our infrastructure partners and key system vendors.

As we work on these four strategic directions: attack prediction, prevention, detection, and mitigation, we will have many opportunities to stretch our capabilities. With respect to all of these, the NIPC is committed to continuous improvement through a sustained process of documenting "lessons learned" from significant events. The NIPC also remains committed to achieving all of its objectives while upholding the fundamental Constitutional rights of our citizens.

The NIPC is also enhancing its strategic analysis capability through the "data warehousing and data mining" project. This will allow the NIPC to retrieve incident data originating from multiple sources. Data warehousing includes the ability to conduct real-time all-source analysis and report generation.

Enhancing Cooperative Relationships Among Federal Agencies

The placement of the NIPC under the jurisdiction of the FBI endows the Center with both the authorities and the ability to combine law enforcement information flowing into the NIPC from the FBI field offices with other information streams derived from open, confidential, and classified sources. This capability is unique in the federal government for reasons of privacy and civil rights.

The NIPC has established effective information sharing and cooperative investigative relationships across the U.S. Government. A written protocol was signed with the Department of Transportation's Federal Aviation Administration (FAA) which will reinforce how information is shared between FAA and NIPC and how that information will be communicated. This protocol documents a long-standing informal process of information sharing between NIPC and FAA. Informal arrangements have already been established with the Federal Communications Commission, Department of Transportation's (DOT) National Response Center, DOT Office of Pipeline Safety, Department of Energy's Office of Emergency Management, and others, which allow the NIPC to receive detailed sector-specific incident reports in a timely manner. Formal information sharing procedures should soon be completed with several other agencies, including the National Coordinating Center for Telecommunications and the Federal Emergency Management Agency's National Fire Administration.

The NIPC has developed into a truly interagency center and this in itself fosters cooperative relationships among agencies. It currently consists of detailee from the following U.S. government agencies: FBI, Army, Office of the Secretary of Defense, Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, General Services Administration, United States Postal Service, Department of Transportation/Federal Aviation Administration, Central Intelligence Agency, Department of Commerce/Critical Infrastructure Assurance Office, and a representative from the Department of Energy. Canada, the United Kingdom, and Australia also each have a detailee in the Center.

The NIPC functions in a task force-like way, coordinating investigations in a multitude of jurisdictions, both domestically and internationally. This is essential due to the transnational nature of cyber intrusions and other critical infrastructure threats.

To instill further cooperation and establish an essential deconfliction process among the investigative agencies, the NIPC asserted a leadership role by forming an Interagency Coordination Cell (IACC) at the Center. The IACC meets on a monthly basis and includes representation from U.S. Secret Service, NASA, U.S. Postal Service, Department of Defense Criminal Investigative Organizations (AFOSI, DCIS, NCIS, USACIDC), U.S. Customs, Departments of Energy, State and Education, Social Security Administration, Treasury Inspector General for Tax Administration and the CIA. The cell works to deconflict investigative and operational matters among agencies and assists agencies in combining resources on matters of common interest. The NIPC anticipates that this cell will expand to include all investigative agencies and inspectors general in the federal government having cyber or other critical infrastructure responsibilities. As we noted on May 22, 2001, the IACC has led to the formation of several task forces and prevented intrusions and compromises of U.S. Government systems. The IACC was instrumental in coordinating the augmentation of the PENTTBOM investigation in the aftermath of the September 11 attacks.

Since 1998, the NIPC has been developing the FBI's Key Asset Initiative, identifying over 5,700 entities vital to our national security, including our economic well-being. The information is maintained in a database 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 CIAO in this regard. Following the September 11, 2001, events and at the request of the National Security Council, the NIPC has leveraged the Key Asset Initiative to undertake an all-agency effort to prepare a comprehensive, centralized database of critical infrastructure assets in the United States.

The NIPC maintains an active dialogue with the international community, to include its participation in the Trilateral Seminar of the International Cooperation for Information Assurance in Sweden and the G-8 Lyon Group (High Tech Crime Subgroup). NIPC has briefed visitors from a number of countries, including: Japan, Singapore, the United Kingdom, Germany, France, Norway, Canada, Denmark, Sweden, Israel, and other nations over the past year. In addition, NIPC personnel have accepted invitations to meet with government authorities in Sweden, Germany, Australia, the United Kingdom, and Denmark in recent months to discuss infrastructure protection issues with their counterparts.

The NIPC sends out infrastructure information to address cyber or infrastructure events with possible significant impact. These are distributed to partners in private and public sectors. A number of recent advisories sent out by the NIPC (see for example Advisory 01-022, titled "Mass Mailing Worm W32.Nimda.A@mm") serve to demonstrate the continued collaboration between the NIPC and its partner FedCIRC. The NIPC serves as a member of FedCIRC's Senior Advisory Council and has daily contact with that entity as well as a number of others including NSA and DoD's Joint Task Force - Computer Network Operations (JTF-CNO).

On issues of national concern, the recent incident involving the Leaves, Code Red and Nimda worms are good examples of the NIPC's success in working with the National Security Council and our partner agencies to disseminate information and coordinate strategic efforts in a timely and effective manner.

Improving Information Sharing

The NIPC actively exchanges information with private sector companies, the ISACs, members of the InfraGard Initiative, and the public as part of the NIPC's outreach and information sharing activities. Through NIPC's aggressive outreach efforts, we receive reports from many ISAC member companies. The NIPC has proven that it can properly safeguard their information and provide useful information in return. This reporting is partially responsible for the issuance of more warning products each year.

Over the past two years the NIPC and the North American Electric Reliability Council (NERC)—the ISAC for the electric power sector—have established an indications, analysis and warning program (IAW) program, which makes possible the timely exchange of information valued by both the NIPC and the electric power sector. This relationship is possible because of a commitment both on the part of NERC and the NIPC to build cooperative relations. In the days following the September 11 attacks, NIPC and NERC held daily conference calls. The close NERC-NIPC relationship is no accident but the result of two interrelated sets of actions. First, as Eugene Gorzelnik, Director of Communications for the NERC, stated in his prepared statement at the May 22, 2001 hearing:

> [T]he NERC Board of Trustees in the late 1980s resolved that each electric utility should develop a close working relationship with its local Federal Bureau of Investigation (FBI) office, if it did not already have such a relationship. The Board also said the NERC staff should establish and maintain a working relationship with the FBI at the national level.

Second, the NIPC and NERC worked for over two years on building the successful partnership that now exists. It took dedicated individuals in both organizations to make it happen. It is this success and dedication to achieving results that the NIPC is working to emulate with the other ISACs.

The NIPC also continues to meet regularly with ISACs from other sectors, particularly the financial services (FS-ISAC) and telecommunications (NCC-ISAC) ISACs, to establish more formal information sharing arrangements, drawing largely on the model developed with the electric power sector. In the past, information exchanges with these ISACs have consisted of a one-way flow of NIPC warning messages and products being provided to the ISACs. However, in recent months the NIPC has received greater participation from sector companies as they become increasingly aware that reporting to the NIPC enhances the value and timeliness of NIPC warning products disseminated to their sector. Productive discussions held this spring with the FS-ISAC, in particular, should significantly advance a two-way information exchange with the financial services industry. The NIPC is currently working with the FS-ISAC and the NCC-ISAC to develop and test secure communication mechanisms, which will facilitate the sharing of high-threshold, near real-time incident information. In the meanwhile we are working with these ISACs to share information. In March 2001, we were commended by the FS-ISAC for our advisory on e-commerce vulnerabilities (NIPC Advisory 01-003). According to the FS-ISAC, that advisory, coupled with the NIPC press conference on March 8, 2001, stopped over 1600 attempted exploitations by hackers the day immediately following the press conference.

Conclusion:

I remain encouraged by the progress the NIPC has made in its first three years. Our multi-agency partnership has developed unique national capabilities that have never before been achieved. We will continually improve in the coming years in order to master the perpetually evolving challenges involved with infrastructure protection and information assurance. Thank you for inviting me here today, and I welcome any questions you have.

STATEMENT OF

SALLIE McDONALD

ASSISTANT COMMISSIONER

OFFICE OF INFORMATION ASSURANCE AND

CRITICAL INFRASTRUCTURE PROTECTION

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

OCTOBER 4, 2001

Good morning, Mr. Chairman and Members of the Committee. On behalf of the Federal Technology Service of the General Services Administration let me thank you for this opportunity to appear before you to discuss our role in Critical Infrastructure Protection.

Background

Critical Infrastructures have long existed in the United States. The shipping systems for the transportation of goods to and from Europe represented a critical infrastructure for our first colonies. In the nineteenth century, telegraph and the railroads became critical infrastructures. As the United States developed an urban, industrialized society, utilities such as gas, electricity and water became critical infrastructures. The difference today is that all of our critical infrastructures now have a common link. Infrastructure systems that were until recently controlled by dedicated computer systems designed and created for one specific purpose are now controlled by applications that run on the same kinds of operating systems that can be found almost everywhere. The development of inexpensive, off-the-shelf computing power and the interconnectivity provided by the Internet have powered our economy, but this same interconnectivity has provided the vulnerability to intrusion and exploitation. Vital systems that control publicly and privately owned and operated critical infrastructures share common attributes that can be analyzed and exploited. The Federal Computer Incident Response Center, (FedCIRC) works to help Federal agencies protect their systems and maintain their critical operations. Other members of the Critical Infrastructure Protection community focus on helping private sector owners and operators to protect their systems and to assure the availability of critical services.

FedCIRC, is a component of GSA's Federal Technology Service. As designated by the Government Information Security Reform Act, FedCIRC is the central coördination facility for dealing with computer security related incidents within the civilian agencies of the United States Government. This Act mandates that Federal agencies report computer security incidents to FedCIRC. Our role is to assist those agencies with the containment of security incidents and to aid them with the recovery process. This directly supports the critical infrastructure protection mission because the Federal Government's agencies depend upon their computer systems not only to conduct government operations, but also to provide vital connectivity to the owners and operators of the Nation's critical infrastructures. For example, the Federal Aviation Administration's networks provide them with critical connectivity to components of the Aviation industry which enabled the FAA to rapidly execute the unprecedented grounding order in response to the acts of terror on the morning of September 11. Similarly, the Treasury Department maintains connectivity to the nation's financial services sector that is crucial to the health of the economy.

When a government agency reports a computer security incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident. Additionally, FedCIRC assists in identifying system vulnerabilities associated with the incident and provides recommendations to prevent recurrence. Upon receiving an incident report, FedCIRC evaluates and categorizes the incident with respect to its impact and severity. If criminal activity is indicated, FedCIRC informs the reporting agency of the requirement to immediately notify Law Enforcement, either their Inspector General or the National Infrastructure Protection Center (NIPC) according to agency policies. If the incident appears to have originated from a foreign country, FedCIRC categorizes it as potentially having national security implications and immediately contacts both the National Security Agency's National Security Incident Response Center (NSIRC)and the NIPC. As appropriate, FedCIRC advises all Federal agencies of the discovery of new vulnerabilities and exploits, and provides guidance to eliminate or reduce the vulnerability, and thwart the exploit.

Incidents involving new vulnerabilities or previously unseen exploits require in-depth analysis. Effective incident analysis is a collaborative effort. Data is collected from multiple sources, then verified, correlated and analyzed to determine the potential for proliferation and damage. This collaborative effort has resulted in the development of an incident response community that includes FedCIRC, the NIPC, the NSIRC, the Department of Defense's Joint Task Force for Computer Network Operations (JTF-CNO), the Intelligence Community's Incident Response Center (ICIRC), industry, academia, and individual incident response components within Federal agencies. Though the respective missions of these organizations vary in scope and responsibility, this virtual network enables the Federal Government to capitalize on each organization's strategic positioning within the national infrastructure and on each organization's unique access to a variety of information sources. Each entity has a different, but mutually supportive mission and focus, which enables the critical infrastructure protection community to simultaneously obtain information from, and provide assistance to the private sector, Federal agencies, the Intelligence Community, the Law Enforcement Community, the Department of Defense and academia.

The NIPC, NSIRC, JTF-CNO and FedCIRC are involved in a constant sharing of sensitive cyber-threat and incident data, correlating it with counter-terrorism and intelligence reports to develop strategic defenses, threat predictions and timely alerts. These efforts depend, not on any one participant, but on the unique and valuable contributions of each organization. The NIPC, because of its relationships with industry, is able to solicit additional participation when dealing with complex analysis issues. This broader spectrum brings together some of the nation's best talent to work on known and developing threats to the cyber infrastructure. FedCIRC's relationship with the NIPC is exemplified by the detailing of FedCIRC staff personnel to the NIPC's Watch and Warning Unit. Alerts and advisories are frequently generated by the NIPC, NSIRC, and FedCIRC as a collaborative effort and represent a consensus when distributed to Federal agencies, industry and the general public.

FedCIRC, NSIRC and the NIPC have initiated a process to improve information sharing and analytic efforts. FedCIRC has developed a standardized reporting format to facilitate joint processing and analysis of incident information. When an incident has the potential for widespread proliferation or damage, the participating organizations routinely pool their information and skills. Cyber-incidents involving a pending or potential investigation are handled in a manner that preserves sensitive cyber-evidence without adverse impact to the affected agency's mission functions or violation of applicable privacy statutes.

The unified response to recent threats to the cyber infrastructure, including the **Code Red Worm**, and the **NIMDA WORM** clearly demonstrate how these collaborative relationships work and how each participant's contributions help to assess and mitigate potential damage. In both instances, industry alerted the incident response community to the new exploit. The Code Red Worm conducted widespread automated network scanning to identify systems operating under Microsoft's Internet Information Server software. A public advisory had been previously released identifying a serious security vulnerability that could allow an intruder to gain control of the vulnerable system and employ it to scan and infect other vulnerable systems. The first version of Code Red commanded thousands of infected computers to simultaneously flood the White House web site, which would result in a denial of service, denying access to citizens seeking information from the White House web site. The attack was thwarted in part by changing the numerical Internet address of the White House web server. This action redirected the attack against a non-existent address, negating any service impact.

During a previous event, a collaborative communication network had been established among the National Security Council, FedCIRC, NIPC, the Commerce Department's Critical Infrastructure Assurance Office (CIAO), NSA, CIA, Department of State, DoD, National Communications System's National Coordination Center (NCC), academia, industry software vendors, anti-virus engineers and security professionals. This network enabled participants to share details as they performed analysis and developed remediation processes and consensus for protection strategies. In the case of Code Red, through the collaboration of the above named groups, the collective team concluded that this worm had the potential to pose a threat to the Internet's ability to function. An unprecedented public awareness campaign ensued, concurrent with efforts to ensure that all vulnerable servers were protected. Statistical information provided by software vendors indicated an unprecedented rush by users to obtain security patches and software updates addressing the vulnerabilities. As a result, the impact of Code Red and its variants was significantly mitigated, and serious impact to Internet performance was avoided.

As this testimony is taking place, collaborative analysis and defensive strategies are being developed for a new and very serious Internet threat, the "**NIMDA Worm.**" Like the Code Red worm, NIMDA self propagates looking for vulnerable systems, but it is much smarter in its quest for victims. NIMDA does not look for a single vulnerability in

Microsoft's Internet Information Server. It attempts to exploit one or more in a long list of know weaknesses and also appends hidden, hostile code to web sites so that any user simply browsing a web site may infect his/her system.

The effectiveness of our response efforts is rooted in our ability to draw on the strengths of our partners and bring to bear the best technical skills against any existing or evolving threat. Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive. FedCIRC, NIPC, NSIRC, DoD, CIAO and industry components are aware that the best response is a proactive, preventative approach. In order to implement such an approach, resources must be focused on the common goal of securing the nation's critical infrastructures and the strengths of each organization must be leveraged in order to achieve the most effective results. FedCIRC, NIPC, DOD, NSIRC, CIAO and others comprise a virtual team, each offering significant skills and contributions to the common defense. These collaborative successes have evolved into a three-tiered collaboration network. FedCIRC, in support of the NSC's then National Coordinator for Security, Infrastructure Protection and Counter Terrorism, has implemented three communication groups dedicated to dealing with Technical Trends; Policy Issues; and Public Awareness Issues. This permits more effective, focused collaboration to take place concurrently, enabling individuals to participate in the groups where their talents are best suited.

Summary

Mr. Chairman, the information presented today highlights the critical and effective relationship that exists between FedCIRC and other members of the Critical Infrastructure Protection community. Though each contributes individually to critical infrastructure protection, our strength in protecting information systems government-wide lies in our collaborative and coordinated efforts. Our missions may appear to overlap in certain areas, but are actually mutually supportive, each focused on a different and critical need. I trust that you will derive from my remarks an understanding of the cyber-threat and response issues and also an appreciation for the joint commitment to infrastructure protection of FedCIRC and the other members of the critical infrastructure protection community. We appreciate your leadership, and that of the Committee, for helping us achieve our goals and allowing us to share information that we feel is crucial to the protection of our nation's technology.

STATEMENT OF JAMIE S. GORELICK
VICE CHAIR, FANNIE MAE

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON GOVERNMENTAL AFFAIRS
342 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, D.C. 20510

OCTOBER 4, 2001

Mr. Chairman, Mr. Ranking Member Thompson and distinguished members of the Committee, thank you for the opportunity to testify today regarding the important subject of protection of the nation's critical infrastructure.

Over five years ago, I testified before this Committee about what was then an emerging issue – the need to protect America's critical infrastructure. Since that time, the Senate Committee on Government Affairs has continued to focus on this important problem, because – as we all know – addressing it responsibly requires a sustained focus and commitment. I commend the Committee for the leadership its members have shown, and share your hope that we can keep our nation and its financial system strong through more effective infrastructure security.

In my testimony in 1996, I raised the specter of a "cyber equivalent of Pearl Harbor," and expressed my hope that we would take active measures to safeguard our country's information infrastructure before such an event. We have, in fact, done much to meet infrastructure security challenges. But in the wake of September 11th, there is a renewed need to assess where we are and where we should be.

So today, I would like to use my time to review the goals we described in 1996, and again, in 1999, in the report of the President's Commission on Critical Infrastructure Protection, and take stock of the progress made toward those objectives. Then, I'd like to offer my recommendations on where we should go from here.

For years, we have known how dependent our nation's security is on the privately held information infrastructure on which it rests. The dependencies on our information infrastructure are increasing daily, as industry – and I speak with particularity about the financial services industry – increasingly operates in a paperless environment. Typically, a large financial institution uses technology to track millions of transactions a day. And each institution is dependent on other networks for its ability to operate. The events of September 11 underscore that dependency. When those buildings were hit, in addition to other tragic consequences, the systems in them and the communications nodes under them went down. With those systems went a large part of the functionality of our financial system. The accompanying malicious code attacks – Code Red, Magistr and NIMDA – caused severe damage to both corporate and government operations.

As we consider our preparedness in light of increased uses and vulnerabilities, we need to ask ourselves two key questions:

1. **Can we detect actual or threatened intrusions into our critical information infrastructures and warn effectively?**
2. **Do we organize and resource correctly to meet the challenges we face?**

Let's first look at the issue of detection and warning. Part of our ability to do this depends on foreign and domestic intelligence-gathering on the intentions, abilities and activities of adversaries and malfeasors. We cannot discuss this question in an open session, but I would give you my assessment that much more needs to be done in this arena.

The other source of intelligence – observed threats and intrusions – are the focus of both public and private sector efforts. When President Clinton issued Presidential Decision Directive 63 (PDD-63), establishing the defense of the nation's critical infrastructures against deliberate attacks, particularly those waged in cyberspace, he presented a rather unique national security challenge, one that the federal government's national security establishment cannot solve alone. With over 90% of the U.S. critical infrastructures being privately owned and operated, assuring the delivery of services vital to the nation's defense and economy must be accomplished in public-private collaboration, with market rather than regulatory solutions being the preferred path.

Let me describe how the financial services industry interacts with the principal government agencies that have responsibility in this area.

The Commerce Department's Critical Infrastructure Protection Office (CIAO) helps proliferate vehicles for private-public cooperation. Let me describe its efforts, as they apply to financial services. Various interested industry participants have, with the support of the CIAO, formed the Partnership for Critical Infrastructure Security (PCIS). The Partnership was intended to be a collaborative effort of industry and government to assure the delivery of essential services over the nation's critical infrastructures. It began as an informal organization, chiefly supported by the CIAO, but it is now a Limited Liability Company with a board of directors, 65 member companies, and an operating budget (through dues collection) of $118,000 dollars. To date, there have been three meetings of the PCIS. More frequent interaction occurs among board members and working group chairs who meet every other week by teleconference to coordinate on-going activities. Recent examples of these activities include industry-sector work on a National Plan, coordinating a media campaign focusing on critical infrastructure protection and information-sharing between sectors and the government. The President of the Board of the Partnership is from CISCO and founding members include PriceWaterHouseCoopers, The MITRE Corporation, Fannie Mae, Bank of America and CitiGroup.

A Financial Sector Information Sharing and Analysis Center (FS/ISAC) has been formed to share information on threats, vulnerabilities and incidents in the financial services industry. The FS/ISAC was launched on October 1, 1999 and became fully operational in January 2000, supported by a trusted third party vendor (Global Integrity, a subsidiary of Predictive). It is a secure facility that provides both authenticated and, where appropriate, anonymous and confidential input. When a member chooses to submit information anonymously, no one will know who submitted the information. Member organizations can enroll by signing an FS/ISAC Membership Agreement and paying an annual fee, based on the organization' requested level of participation.

The FS/ISAC is:

- A private sector partnership among eligible financial services providers
- A database owned by the membership and managed a third party
- An anonymous submission facility for security incidents and transmission system for alerts of serious incidents
- A database structured to allow members to search for incidents, vulnerabilities, threats, and solutions, available and operated 24 hours per day, 365 days per year.

Member organizations include insured depository institutions, securities firms, investment companies, insurance companies, credit card companies, government-sponsored enterprises, clearing and settlement entities, and providers of financial technology. FS/ISAC members account for eight of the top ten commercial banks, seven of the top ten securities firms, over 80 percent of the total commercial bank assets, and over 80 percent of assets under management by the top 50 open end investment companies.

All this is good progress since the CIAO was established, but the scope and scale of our capacities are not where they need to be for us to meet the challenges we face now. The PCIS and the ISACs are volunteer-based organizations that are, for the most part, not well-known, well-funded or well-staffed. For example, while the FS/ISAC has a third-party provider who convenes members for twice yearly meetings, there is limited infrastructure for real-time communication, no emergency planning other than on a volunteer basis, and limited operational capacity to act in an emergency.

Other ISACs may be farther along. I understand that the National Energy Regulatory Council, which has become the ISAC for the electric industry, has twenty-one security coordinators in the network, available seven days a week, twenty-four hours a day (though it does not have an actual operations center). I also understand that the National Communications Center (NCC), the ISAC for the communications industry, is co-staffed by both government and industry representatives and has a truly operational capability. In addition, an Alerting & Coordinating Network (ACN) was established to link all of the NCC control centers together. All of the operation centers for various companies can communicate with each other through the ACN. Because the NCC is staffed on a full-time basis, it is able to make better progress with information-sharing. For example, it has established Concept of Operations and Participation Criteria and has made a vigorous effort to reach out to other ISACs like the FS/ISAC. An Information Sharing and Analysis System used for emergency communications was accredited this April.

In addition to the above activities, government-sponsored Computer Incident Response Teams (CIRTs) have been organized to handle computer security related incidents, such as incident detection, incident containment and incident recovery. These include the Department of Defense's Joint Task Force – Computer Network Operations Center (JIF-CNO); the Carnegie Mellon - Computer Emergency Response Team (CM-CERT); the National Security Incident Response Center (NSIRC); and the Federal Computer Incident Response Center (FCIRC). Each of these has a particular focus, e.g., on the protection of defense establishments or the provision of alerts to federal agencies, etc. Information-sharing between government organizations and industry ISACs is done on an individual basis. The PCIS has established a Task Force to develop a common taxonomy and architecture to standardize information-sharing between these government organizations and industry.

I said at the time of the President's Commission report that industry needs help in establishing the infrastructures for sharing information, developing protection standards, and issuing warnings. It has become even more clear since then that these structures do not evolve on their own and, if they do evolve, they may do so on a time-table that does not match our national security challenges. The differences among industry sector ISACs appears to correlate, in part, with the degree of governmental support or involvement, and also whether these were pre-existing industry groups that could take on this task. Each of the relevant government agencies should be responsible for affirmatively helping industry stand up and staff a structure that can bring all industry participants and relevant government participants together to meet these tasks.

Each ISAC also needs to have relationships with the others and with the various government cyber warning and analysis centers. Progress toward this goal is highly uneven and inadequate. While, for example, the information-sharing between the NIPC and the NERC is reportedly robust, the relationship with other ISACs reportedly is not as strong. The communications among ISACs is spotty at best.

The FBI's NIPC has done a good deal of work in its InfraGuard system to build trust with and to exchange information with industry. It now has 1800 member companies, including Fannie Mae. There are two impediments to its effectiveness: reservations in industry about sharing information, and resources.

Two changes in the law, previously recommended, should be considered again to increase the flow of information. The Freedom of Information Act contains many exceptions, but none protects from disclosure information that a company provides about its own vulnerability. I understand that the proposed Davis-Moran Act is one idea of how to provide some level of protection for private sector companies that voluntarily provide cyber-security information to the government.

Similarly, there evidently remain antitrust concerns limiting both the sharing of information and the development of common standards by companies working in concert. As well, there are liability concerns limiting the use of cyber-security audits and tests. The industry experts who are working on these issues can, I am sure, address the Committee's interest in these issues.

There would also, I believe, be more information flowing to the FBI about attempted intrusions if companies thought that the FBI could or would investigate the repeated "pinging" of a system, by which someone is clearly looking for entry points or vulnerabilities. To me, "pinging" is like walking around a neighborhood trying all the doors and windows. We should not consider this activity to be benign. Right now, a private company can go no further in protecting itself from a concerted effort to enter its system than to politely inquire of the Internet Service Provider from which the "pinging" emanates if it might look into the matter. The government cannot take action until the intruder has gotten through the door. It is therefore fruitless to share that information with the government.

While the government has significantly improved its ability to investigate cyber attacks, it does not appear to have adequate resources. In 1998, the FBI established a nationwide capability to investigate computer attacks, the "National Infrastructure Protection and Computer Intrusion Program," under the program management of the NIPC. The NIPC has established guidance and training curricula to build a cadre of trained investigators. The number of cases more than tripled over the last three years, to over 1200 pending investigations. In addition, the NIPC built a core of computer scientists to assist on the most complicated investigations.

But the FBI has a substantial backlog of investigations in this area, so that even if it has information about a threat or intrusion, it cannot consistently follow through to investigate. With a staff of 200 agents in this area, the FBI cannot do all the things we have asked it to: investigate actual incidents, establish InfraGuard chapters, set up data bases of 'key assets', man the detection and warning functions, etc. I would suggest that this Committee evaluate the adequacy of the resources that we apply to the protection of our national information infrastructure.

Neither the NIPC nor the Commerce Department, nor anyone in or outside of government, has the operational capacity or authority to coordinate the actions of industry in an emergency or to recover and reconstitute critical infrastructures debilitated or destroyed by an attack. The original theory was that this was primarily the responsibility of the private owners and operators of those systems. Even if that is so, someone must lead the effort. Each "lead agency" of the government charged with responsibility for each infrastructure section (Energy for electrical power; Transportation for oil and gas; Treasury for banking and finance, etc.) was supposed to develop a recovery and reconstitution plan in concert with the relevant sector. As I understand it, to date, only the NIPC and its sector, Emergency Law Enforcement Services, have developed a plan. Others have works in progress. So we do not have extant plans for recovery. We should have such plans and the capacity to limit the impact of a successful cyber intrusion, as well as the capability to work around it to keep the system running. We also need to be able to counter-attack when privately held computer systems are attacked. We have seen that terrorists understand the attractions of both governmental and private sector targets, but are we prepared to respond to an attack on these non-military targets, to fight back to prevent further damage?

Finally, as in so many issues, the many and varied responsibilities of organizations in this area could benefit from clarification to reduce redundancy and turf battles. Responsibility for the identification and the planning for protection of 'key assets' resides in the FBI's NIPC, the Commerce Department's CIAO and, as the Defense Department moves closer to a homeland security role, likely there as well. Those of us who help run key assets need to know with whom to work.

Because the framers of PDD-63 were concerned that industry would reject a government-led effort, it encouraged the proliferation of private groups to do the work that needed to be done. But now, there are the CIAO, the NIPC, the PCIS, the many ISACs, and the many CIRTs. It would be helpful to take stock, clarify and, if necessary, streamline and strengthen the structure so that it is truly robust.

That brings me to the second key question:

Do we organize and resource correctly to meet the challenges we face?

There are many, many willing partners in the private sector in this important work. For our own business continuity, we need to protect our own infrastructures and help our business partners do the same. But we are unused to collective or collaborative action like that called for here. We also have a great deal of technical expertise to share, but we are used to protecting, not sharing, our technical prowess. The ISACs and the PCIS provide for such activities, but we would be helped if we had:

- coherent, cohesive leadership from the government and a clear understanding of who is doing what in the government
- adequately resourced support for the establishment of robust infrastructures like the ISACs that convene industry participants, share information and plan for an emergency
- a legal rubric that makes it easier to share information and set common standards
- a robust set of investigative resources to whom we can turn when there is evidence of an intrusion or threat of one
- and, in an emergency, a plan and a person or persons with authority to act on that plan.

With continued focus on the importance of these efforts, together we can better protect our critical information infrastructure.

Thank you for the opportunity to appear before you today.

TESTIMONY OF

Joseph P. Nacchio
Chairman & Chief Executive Officer
Qwest Communications International, Inc.

Before the Senate Governmental Affairs Committee

October 4, 2001

CRITICAL INFRASTRUCTURE PROTECTION: WHO IS IN CHARGE?

Good morning, Mr. Chairman and Members of the Committee. It is an honor to be here this morning to share Qwest's views on this subject of paramount national importance. Thank you for holding this timely hearing and for including us among these distinguished panelists.

Let me begin by briefly introducing my company and myself.

Qwest is a four-year old Fortune 100 company, with 66,000 employees and annual revenues of over $20 billion. We are a telecommunications company of the 21st century, providing local and long distance, telephone, wireless, and Internet web hosting services over a state-of-the-art network to homes, businesses, and government agencies in the United States and around the world, including the US Departments of Defense, Energy, and Treasury.

Although I am here today in my capacity as Chairman and CEO of Qwest, I also serve as Vice Chair of the National Security Telecommunications Advisory Committee, often referred to as NSTAC. NSTAC is an organization of 30 CEOs from the telecommunications, technology and other industries who share information about emergency preparedness and advise the President and other White House leaders on a wide range of national security and related concerns. I bring to this organization, and to the Committee today, my thirty years' experience in the telecommunications industry, particularly on issues relating to information security and critical infrastructure protection.

Mr. Chairman, two weeks ago the President reassured the nation that the state of the Union is strong. This morning I offer you the same assurance regarding the nation's telecommunications infrastructure.

America's telecommunications infrastructure is the best in the world, and the engineers, technicians, and workers who maintain it are second to none in their technical ability and selfless dedication. We saw the proof on September 11. Despite the horrific damage sustained at the World Trade Center and at the Pentagon, the nation's telecommunications infrastructure continued to operate. It brought us the sounds and images of tragedy, it summoned emergency rescue services, and it alerted our military forces.

At Ground Zero in New York, telecommunications companies put aside their everyday marketplace rivalry and came together as one to help restore communications in lower Manhattan. For example, Qwest immediately diverted a multimillion-dollar shipment of switching equipment to lower Manhattan, gave top priority to any and all requests from emergency service providers engaged in rescue and recovery efforts, and provided free Internet connections and services to those who had lost them. Similar efforts were made by many other telecom companies -- a collaborative industry undertaking praised by FCC Chairman Michael Powell as "heroic efforts…insuring that the world's premier communications network has continued to be available in this time of tragedy."

I stress this point because, where some have focused on how *vulnerable* our networks are, we must also remember how *resilient* they are. In this sense, our networks' performance during and after this indelible national tragedy can teach us some valuable lessons about the control and protection of critical infrastructures that the Committee is asking this morning.

First and foremost, the telecom industry understands that our networks are, quite literally, the conduit that connects the other essential sectors of our economy. For that reason, we understand that we bear a unique responsibility in being the first line of defense in protecting our own infrastructure. Keeping both our *internal* and *external* networks safe is something that companies in the telecom industry do every day — and will continue to do in the future.

Let me give you two examples of this from our own experience. First, to defend our *internal networks* from both physical and cyberattack, Qwest has implemented a comprehensive information network security program, which includes classification of network assets, the development, implementation and monitoring of a complete set of security policies and procedures, extensive employee training, and a plan for disaster response and recovery. Qwest's security program serves as a model for other companies, and will shortly be recommended for adoption by all NSTAC industry members. Second, to protect our *external networks*, just last month Qwest dedicated more than 1,000 technical experts to assist our customers affected by the global "Code Red" computer virus. Such a quick and comprehensive response to threats to network operations has become a necessity.

But, in all candor, it's not enough. Other industries need to take similar steps to protect their own critical infrastructures. Communications providers know from experience that any network is only as strong as its weakest link, and we can only protect communications networks up to the point of service. Vulnerable infrastructure in any industry affects all industries. A communications provider can have the most secure network in the world, but if other industries we serve have vulnerable infrastructures, our networks may continue to be open to attack. In other words, *each* company must therefore protect *its* own critical infrastructure; and *all* companies, whether managing and operating critical infrastructure or running traditional business operations, have a responsibility to exercise prudent risk management.

Private sector companies are in charge of protecting their corporate assets, including digital data and networks, physical facilities, and people. Officers and directors have a fiduciary duty to their shareholders to protect corporate assets and operations. This means they must take security of their data and networks seriously. Quite simply, corporate America must begin to exercise oversight, effectively manage infrastructure risks, institute corporate security plans, adequately fund security initiatives, and look for ways to collaborate on critical infrastructure protection.

The public sector and its agencies have additional responsibilities as well. I'll briefly mention three. First, as in business itself, a major aspect of communications network design is risk management. When designing a network, agency mission and objectives are calibrated to reflect the acceptable level of risk. As of September 11, the definition of acceptable risk was dramatically changed, and such concepts as the need for redundancy, single point of failure, and the reliability of a network now need to be redefined.

Second, increased standardization of security requirements across the agencies is crucial. Terms like "redundancy," "single point of failure," and "reliability" need to be precisely and uniformly defined. Presently, agencies interpret these terms differently and leave it to the vendors to attempt to discern their intent. Also, with "lowest cost" evaluation models the government often inadvertently encourages vendors to shortchange security requirements to minimize their bids and then perhaps "evolve" their proposals to deal with the technical security issues after contract award. Obviously, such an approach leads to no consistency across the government in its ability to resist or respond to network attacks. Standardization cries out for attention.

Finally, the Government must take steps to increase the sharing of information. During the recent crisis, the efforts of NSTAC and the National Coordination Center demonstrated that one of the best means to defend against terrorists is the timely and accurate sharing of information. Private sector companies should not be subject to FOIA requests or other exposure from the Government, investors or competitors for helping to protect critical infrastructure. Appropriate legislation should be crafted to protect companies similar to the legislation that was developed for the Y2K problem.

This brings me to the issue of how companies and the public sector can jump-start their efforts in the face of this national emergency. Here again, the telecommunications industry's longstanding history of shared responsibility and cooperation provides a model to follow.

NSTAC has been key in furthering shared industry responsibility and private-public sector cooperation. In terms of facilitating interindustry efforts, NSTAC studied Qwest's internal network security program, and has recommended that all its member companies adopt it to safeguard their own networks. And during the unfolding tragedies on September 11 NSTAC's National Coordinating Center and its Information and Analysis Center for Telecommunications operations, supported by many of our members, played a pivotal coordinating role in restoring telecommunications services and providing essential communication needs in both New York City and at the Pentagon.

How can we best build on the current framework to broaden its scope and increase its effectiveness? There are several interrelated ways of doing this. For example, NSTAC and the National Security Council should immediately initiate a project to develop benchmarks and requirements for Information Security Best Practices for the telecommunications industry. Either NSTAC or a public organization, such as the National Infrastructure Simulation and Analysis Center proposed by Senator Domenici, could be given the responsibility to extend these clearinghouse and coordination functions to other industry segments as well.

No matter what organizational structure you establish to carry out these expanded planning and coordination functions, it will not succeed if existing law works against the ability of companies and government to freely share sensitive information on infrastructure protection. Legislation introduced recently by Senators Bennett and Kyl recognizes this. Congress should remove real or perceived barriers to information sharing in order to allow the exchange of critical information about infrastructure threats and assure that the information exchanged will not, directly or indirectly, fall into the hands of our enemies. And Congress should complement these efforts by enacting legislation increasing the penalties for cyberattacks and acts of vandalism that impair the telecommunications infrastructure, and by giving law enforcement greater latitude to investigate and prosecute these attacks.

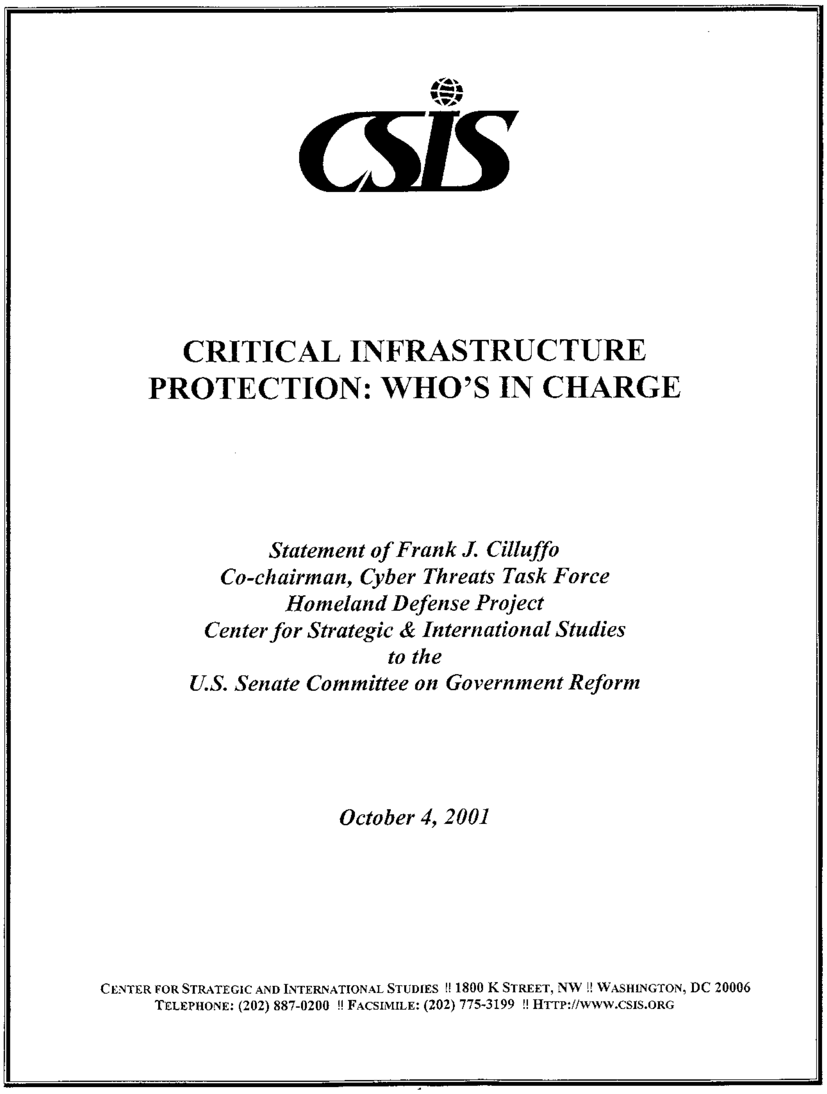
I'm a businessman, not a lawyer, so I won't presume to advise you about the privacy and other legal ramifications of the information sharing and wiretapping legislation Congress is now considering. But as a telecom executive I can assure you that our networks are sound and ready to help preserve our national security.

Conclusion

In my testimony I have stressed several points: *first,* telecommunications companies have a critical responsibility to defend their internal and external networks against physical and cyberattack, and to adopt policies and procedures that will do this; *second,* all companies must strive to ensure the security of their data and networks; *third,* interindustry coordination and industry/government cooperation are essential to these efforts; and *fourth,* there are a number of steps that Congress should take to enable these efforts to be both broader and more effective.

And now let me conclude. I began by saying that our country's telecommunications infrastructure is strong — and it is. But it can, and must, be stronger. I speak for Qwest, and without doubt for the rest of our industry, when I commit to you that we will do whatever is necessary to work with this Committee and the Congress to assure the continued strength of the networks that make up America's telecommunications infrastructure.

####



CSIS

CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE

Statement of Frank J. Cilluffo
Co-chairman, Cyber Threats Task Force
Homeland Defense Project
Center for Strategic & International Studies
to the
U.S. Senate Committee on Government Reform

October 4, 2001

Center for Strategic and International Studies !! 1800 K Street, NW !! Washington, DC 20006
Telephone: (202) 887-0200 !! Facsimile: (202) 775-3199 !! http://www.csis.org

Chairman Lieberman, Senator Thompson, and distinguished committee members, it is a privilege to appear before you today to discuss this important matter. I would like to commend you for squarely facing this complex challenge.

In the wake of the terrorist attacks on the World Trade Center and the Pentagon, the United States is confronted by harsh realities: Our homeland is vulnerable to physical attack, gone is the sense that two oceans provide protection. But this is not only a US problem. In many ways it was a blast heard round the world, the reverberations of which will be felt for years to come.

It is widely accepted that unmatched U.S. power (economic, cultural, diplomatic, and military) is likely to cause America's adversaries to favor "asymmetric" attacks over direct conventional military confrontations. These strategies and tactics aim to offset our strengths and exploit our weaknesses.

The terrorists attacked highly visible symbols not only of our military strength, but also of our economic prowess. Though exceedingly well planned, coordinated, and executed, the comparatively low-tech means employed by the terrorists raises the possibility of a well placed bomb, a cyber strike, or worse yet a more inclusive, more sophisticated, assault combining both physical and virtual means on one, or several, critical infrastructures. The window of opportunity for implementing a comprehensive course of action that will remedy existing shortcomings is rapidly closing.

As we will never be able to protect everything everywhere all the time from every enemy – at least not in a democracy such as our own – now is the time for clearheaded prioritization of policies and resources. Unless we examine the problem in its totality, we may simply be displacing risk from one infrastructure to another. We need to approach the problem holistically, examining the dangers posed to our critical infrastructure in both the physical and virtual worlds and where they converge.

Infrastructures have long provided popular terrorist targets: telecommunications, electric power systems, oil and gas, banking and finance, transportation, water supply systems, government services, and emergency services. Destruction or incapacitation of these systems could have a debilitating effect on US national and/or economic security. This is a brief sampling of terrorist attacks on critical infrastructures intended to frame an historical context for the discussion.

Telecommunications

- In 1987, the LTTE attacked a telecommunications complex north of the Jaffna tower, severely damaging or destroying the sophisticated computer systems housed there. This was part of an overall campaign to deprive the residents of Jaffna of basic amenities, including public libraries and telephone services.

Electric Power Systems

- In 1997 IRA terrorists sought to bomb 6 National Grid Group sub-stations, which would have cut off all power to the city of London and the south-east. Had this plot succeeded, it would have crippled hospitals, transportation, emergency services, and vital computer links and would have taken months to return full service. A joint operation by MI5, Special Branch, and the Anti-Terrorist squad thwarted the plan and resulted in the arrest of top IRA conspirators.

Oil and Gas

- In July 1996, Scotland Yard foiled an attack by the IRA directed against gas and water plants in London. The police arrived "in the nick of time," arresting seven people and confiscating 180 pounds of semtex.
- Over a year and a half period between 1997 and 1998, there were more than 160 attacks on Canadian gas wells, pipelines, and businesses. Terrorists have struck with various sorts of artillery, bullets, and bombs.
- In 1999 there were 132 terrorist attacks against transportation, 16 more then the year before. Of these pipelines lead the list, accounting for 78% of the total.
- The FARC and the ELN have had great "success" in targeting Colombia's oil and gas pipelines. According to the most recent State Department study, *Patterns of Global Terrorism*, in 2000 the ELN carried out the majority of the 152 attacks against the Cano Limon, Columbia's second largest crude oil pipeline. As a result, Occidental Petroleum had to halt exports through most of August and September.
- The retarded growth of the Russian pipeline illustrates how these security concerns can severely impact not only established structures but also the development of new ones.

Banking and Finance

- In 1992, the IRA bombing of London's Baltic Exchange cost three lives and caused over $1 billion in damage.
- Building off of this model, they struck again in 1993, bombing London's "Square Mile, England's financial center, again inflicting over $1 billion worth of damage. This bomb, detonated over the weekend when casualties would be low, targeted British economic strength.
- In April 1996, the LTTE drove a truck laden with explosives into the Central Bank in Colombo, the capital of Sri Lanka, killing 91 people.

Transportation

Air

- In July 22, 1968 the Popular Front for the Liberation of Palestine (PLFP) highjacked an El Al flight. With the 1972 attack on Ben-Gurion airport, terrorists graduated from attacking airplanes to indiscriminate bombings.
- With focused efforts and diligence, the number of attacks decreased, even as the overall number of terrorist incidents has increased – demonstrating the value and possibility of hardening targets. The hijacking of Air France Flight 139 in July 1976 by terrorists, and its subsequent re-routing to Entebbe, Uganda, prompted a highly successful raid by an Israeli commando team. In the end, the hostages were freed, no ransom was paid, and the terrorists' demands went unmet.
- In October of the following year, four terrorists (led by Zohair Youssef Akache) hijacked a 737 bound for Germany from the Balearic Islands. After flitting around Europe and the Middle East, the plane was finally landed in Mogadishu, Somalia. While there, the "crack" German anti-terrorist unit GSG-9, along with two British Special Air Services members on loan, successfully stormed the aircraft and rescued the hostages. Here too, the situation was resolved by the use of force without payment of ransom. Following these two successful counter-terrorist operations, terrorists changed tactics, moving away from hijacking aircraft to bombing them.

Railroads and Trains

- In 1995, an unknown group calling themselves the "Sons of Gestapo" derailed an Amtrak train, causing it to plunge off a 30-foot high bridge and crash into a dry streambed 50-60 miles from Phoenix, Arizona, by removing 29 spikes from the track.
- Also in 1995, Aum Shinrikyo carried out their sarin gas attack in the Tokyo subway system. Not only is this attack significant because of it was an attack on the transportation but also because it was the first indiscriminate use by a terrorist organization using a chemical nerve agent.
- Even threats can have a substantially disruptive effect. In April, 1997 IRA bomb threats alone shut the city of London down. The IRA detonated a real bomb at the Leeds station, without injury. They then made a series of calls using the code words designed to inform the police that it really was an IRA member on the line, and shut down the King's Cross, St. Pancras, Paddington, and Charing Cross rail stations, the Jubilee subway line, numerous streets around Trafalgar Square, Gatwick and Luton Airports were entirely closed, and Terminal Three at Heathrow was closed temporarily. In essence, the IRA managed to shut London down by the mere threat of violence.
- Just last week, a bomb aboard the North East Express, traveling between New Delhi and Gauhati, India derailed seven cars and injured 100 people. Though no group had claimed responsibility, authorities believe it to have been the work of the National Democratic Front of Boroland.

Maritime

- In October 1985, four Palestinian terrorists hijacked the cruise ship Achille Lauro and her 750 plus passengers. They killed American Leon Klinghoffer, and then violently threw his body and his wheelchair overboard. Egyptian and PLO officials managed to negotiate a deal with the terrorists in which they would be granted safe passage from Egypt if they surrendered the ship and her passengers. While en route, US fighter planes intercepted the plane, forcing it to land

- Piracy accounts for 28% of the worldwide violent attacks carried out against transportation in 1999, up 36% from the year before. Considering that 85% of the world's good travel by ship, those figure add up to substantial losses in a hurry.
- In October of 2000, suicide bombers used a shaped charge mounted on a skiff to kill 17 US sailors and wound 39 others aboard the USS Cole while at port in Aden, Yemen. The bombing of the USS Cole continues to serve as another grim reminder that terrorists will continue to probe and will strike where they can.
- Also in October 2000, the LTTE mounted a well-organized attack on Trincamalee harbor, injuring 40 people and destroying two crafts by guns and a large passenger craft by explosion. These attacks are part of the overall attack and looting campaign carried out by the Sea Tigers, the LTTE's naval branch.
- The fall 2000 report of the Intertagency Commission on Crime and Security in U.S. Seaports highlighted that in terms of the threat posed by terrorism "their vulnerability to attack is high" and "such an attack has the potential to cause significant damage."

Water Supply

- In October 1987, a teenager threatened to blow up the Bonneville Dam on Washington state's Columbia River unless he received $15,000. An FBI agent shot and killed him. The "detonator" turned out to be a cell phone.

Emergency Services

- In 1996, a Swedish man disabled portions of the US emergency 911 system in Southern Florida from his home in Goteburg.

And the list goes on. These examples only begin to plumb the depth of what we have already seen and intimate what is possible. What if the terrorists had decided to crash one of the planes into a nuclear power plant, a liquefied natural gas plant, or an oil refinery? There would be many more potential casualties as well as the dangers posed by environmental concerns. The Nuclear Regulatory Commission stated that America's nuclear reactors would not be able to sustain an impact from an airplane used of the kind used in the September 11th attacks. Thirty-one states have nuclear power plants that supply about 20 percent of the nation's electricity supply. If one of these was hit not only would we need to deal with the interruptions of electric power, but also with the cleanup and pollution from the damaged reactor.

Bits, bytes, bugs, and gas will never replace bullets and bombs as the terrorist weapon of choice. Al Qaeda in particular chooses vulnerable targets and varies its *modus operandi* accordingly. They become more lethal and innovative with every attack – the first attempt on the World Trade Center, the Khobar Tower, the U.S. embassies in Africa, the

USS Cole. In light of this demonstrated escalation and flexibility, we must shore up our vulnerabilities, and cyber threats are a gaping hole. While bin Laden may have his finger on the trigger, his grandson may have his finger on the mouse. Moreover, cyber attacks need not originate directly from al Qaeda, but from those with sympathetic views.

For too long our cyber security efforts have focused on the "beep and squeak" issues, and have been attracted to the individual virus or hacker in the news, often to the neglect of the bigger picture, incorporating the economy and beyond. It is time to identify gaps and shortfalls in our current policies, programs, and procedures, begin to take significant steps forward, and pave the way for the future by laying down the outlines of a solid course of action that will remedy existing shortcomings. Along these lines, there have already been a series of actions taken, some prior to September 11 and some post.

In particular, I applaud the creation of the new cabinet level Office of Homeland Security, directed by Pennsylvania Governor Tom Ridge. It is my understanding that a comprehensive review will be completed by next week, which will set out the office's roles, missions, and responsibilities. We will then have a better sense of the explicit roles and responsibilities pertaining to homeland security and how they pertain to critical infrastructure protection – perhaps most notably continuity of operations and continuity of government missions.

This attack was a transforming event. We cannot examine past precedent as to what had and had not worked before because we now have a new frame of reference, one that requires a new outlook. Because this is a top priority issue, organizational charts, titles, and line items, historic emblems of bureaucratic power, fade into the background. Governor Ridge will have the ammunition required to carry out his mission because it has the full confidence and backing of the President. But even an undertaking of this importance takes some time to move from concept to capability. Once the immediacy of the problem has settled into routine, several months hence, we should consider codifying and institutionalizing its mission with congressional legislation and additional statutory authority if needed.

Prior to the events of 11 September, the executive branch was drafting a new National Plan and Strategy to provide guidance and direction for cyber security, scheduled for release by year's end. Likewise, an Executive Order (EO) on the same subject, entitled "Critical Infrastructure Protection in the Information Age," was near completion and efforts are underway to ensure that it jibes with the other initiatives. And, in his first National Security Presidential Decision (NSPD 1), promulgated on March 5, 2001, President Bush emphasized that national security also depends on America's opportunity to prosper in the world economy. Indeed, cyber security lies at the core of our economic prosperity, which is our "nerve center" – and President Bush and his team should be congratulated for having taking new steps on this front.

As both the Executive branch and Congress consider how best to proceed in this area, we should not be afraid to wipe the slate clean and review the matter with fresh eyes. We need to be willing to press fundamental assumptions of national security. Cyber threats and information assurance are cross-cutting issues, but government is organized along vertical lines. Though it is crucial to conduct our review with a critical eye, it is equally important to adopt a balanced viewpoint – one that appreciates both how far we have come and how far we have to go.

Fortunately, centers of excellence do exist – both in government and the private sector - and we should leverage and build on them. Only now, with the requisite amount of water under the proverbial bridge, have we amassed sufficient knowledge and experience to formulate the contours of a comprehensive cyber security strategy. It is essential that any strategy encompass prevention, preparedness and incident response, vis-à-vis the public and private sectors, as well as the interface between them.

Such a strategy would generate synergies and result in the whole amounting to more than simply the sum of the parts (which is not presently the case). Such an approach would also offer enhanced protection for the "nerve center" that is the U.S. economy.

A Brief Snapshot

Information technology's impact on society has been profound and touches everyone, whether we examine our economy, our quality of life, or our national security. Along with the clear rewards come new risks and a litany of unintended consequences that need to be better understood and managed by our industry and government leaders.

Unfortunately, our ability to network has far outpaced our ability to protect networks. The events of September 11 are a marked counterpoint to the daily invasion through cyberspace. There is no shortage of examples of our vulnerability, based on past red team exercises. Likewise, demonstrated capabilities – fortunately, without truly nefarious intent – are also in evidence. Already, we have seen a young man in Sweden disable portions of the emergency 911 system in Southern Florida and a Massachusetts teenager disable communications to an aviation control tower.

Fortunately, however, we have yet to see the coupling of capabilities and intent (aside from foreign intelligence collection and surveillance), where the really bad guys exploit the real good stuff and become more techno-savvy. It is only a matter of time before the convergence of bad guys and good stuff occurs. We must develop the means to mitigate risk in an electronic environment that knows no borders.

Against this background, we need a true national debate on infrastructure assurance, and we need to re-think national security strategy – and, by extension, economic security and our nation's security – accordingly. It can no longer be a case of the government leading and the private sector following. In other words, Silicon Valley and the Beltway, where the sandal meets the wingtip, must stand side by side and on equal footing in addressing these issues and formulating responses.

As to the specific question of "who's in charge", this is a shared responsibility between the public and private sectors.

Building a Business Case

Government, industry, and individuals all have leadership roles to play. Cyber security and its implications for economic security represent twenty-first century challenges. Twentieth century approaches and institutions simply will not work. Instead, we need new organizations, novel management practices, and an array of new tools. Though this is not an area where government can go it alone, it can – and must – set a good example. In fact, only through leading by example can the government realistically hope for the private sector to commit the sort of effort – in time and resources – expected of them. And we need to be sure and set the bar high.

But, while government is eminently well suited to do certain things, others are best left to industry to do. Put another way, just as important as identifying what government should do is identifying what it should not do. What follows below is an attempt to put flesh on these skeletal statements in so far as they relate to cyber security and its implications for economic security.

Before proceeding to focus on sector-specific (that is, public and private) strategies, however, I would like to briefly lay out a few general guiding principles. In particular, a solid approach to critical infrastructure protection and information assurance (CIPIA) must, in my view, be centered on three "prongs," namely: policy, technology and people. Underpinning this triadic structure must be education and awareness, and superseding it must be leadership. Without leadership, the entire structure crumbles because policy priorities are only sustained if political will and the necessary resources support them.

Improving the Public Sector's CIPIA Readiness

The starting point for the discussion here must surely be Presidential Decision Directive 63, the May 1998 directive that established the framework for tackling the critical infrastructure/cyber security issue. Among other things, PDD-63 established the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Assurance Council (NIAC), as well as identifying the "National Coordinator" (at the NSC) as the central coordinating figure for the federal government. The PDD laid out aggressive goals for improving federal systems, incident warning and analysis, research and development efforts, IT security worker skills, and cooperation among federal agencies and with the private sector. Unfortunately, this directive has proved to be long on nouns and short on verbs. Put another way, planning is everything – plans are nothing. The time has come for implementation and execution.

But planning, implementation and execution are all complicated by the fact that the government is presently organized along vertical lines – even though cyber security constitutes a cross-cutting mission. Among other things, this makes it difficult to assure accountability. Against this background, we need to streamline and re-adjust the workings of our public sector, and coordinate its constituent components so as to increase efficiency, clarify responsibilities and heighten accountability – all the while bearing in mind that outreach to the private sector is equally critical.

Successes enjoyed to date were often in areas without significant budgetary implications or where the need for change was so compelling that some work had to be accomplished. Without strong budgetary authority residing in the National Coordinator, many important items could not be accomplished and, among other things, this made it very difficult to assess responsibility or accountability when CIPIA readiness failed.

On a positive note, the Department of Defense (DOD) and Intelligence Community have established a level of information assurance readiness that is typically much more mature then their civilian agency counterparts. This is to be expected, as they have experienced the impact of cyber attacks over the past decade and experienced many of their own vulnerabilities. The rest of the federal government will continue to benefit from these DOD experiences and the solutions that DOD has crafted for itself. These provide building blocks for the government to develop its cyber security strategy.

The government must lead by example. Without first having its own house in order, it cannot provide the private sector with the necessary support or encouragement essential to promoting strong CIPIA. Seven recommendations for action in the federal government follow.[1]

(1) **Leadership**. Critical to the federal government effort is having at its apex a single individual or group endowed with the requisite powers and responsibilities to make the system work. To this end we need to appoint a senior government official with clout or "teeth" - that is an Assistant to the President for Information Security – whose efforts are supported by the White House. This senior official would have a small staff and use an interagency working group to coordinate federal agency efforts and programs. This position should be confirmed by Congress and among other things would be empowered to issue directives regulating the security of federal agencies IT systems; would hold budget review authority on those portions of a federal agencies budget concerning information technology or critical infrastructure to ensure sufficient security funds are requested; and would conduct audits/assessments to ensure federal agency accountability and adherence to IT security standards. This senior official would be responsible for reporting to the President, and to the Congress, on the performance of individual agencies.

In addition, this senior official would be responsible for developing an annual plan to identify crosscutting issues, have a limited budget to begin to develop crosscutting government-wide solutions, and ensure sufficient research and development efforts are undertaken.

[1] These recommendations are drawn from a forthcoming Joint Economic Committee report authored by Mark Montgomery and myself.

The foregoing proposal, with its centralizing features, is intended to streamline and replace the myriad of structures that currently exist. Notably, a similar motive apparently underlies the Executive Order that is currently being formulated. There is a good chance that the EO will establish some sort of a board, including a number of federal agencies and organizations, with a chair and a vice chair from the private sector, with an eye towards clarifying and delineating responsibilities in the area of cyber security, and heightening accountability. This may have two chains of command – one through the National Security Advisor and the other through the Director of the Office of Homeland Security.

(2) **Risk Mitigation**. A key element in improving the computer security of federal agencies is the need to rapidly respond to incidents or threats and repair known software faults. The federal government must implement a system to provide real time information assurance vulnerability alerts to system administrators, identifying possible attack techniques or targets and known threat ISP addresses. This system, which could leverage the less robust FEDCIRC system already in-place at GSA, must be fully connected to the defense department, intelligence, and law enforcement warning systems and must also maintain good communications with private sector operated warning centers.

An equally important risk mitigation effort in the federal government is the efforts to rapidly identify, distribute, and install software "patches" which are developed by vendors to correct known flaws in operating system codes. The time period between the distribution of the patch by the vendor and the installation of the patch by the system administrator is the most vulnerable time for an operating system, and the pace of this installation must be increased. Additionally, the federal government must work hard on the development of automated tools to help with both vulnerability alert distribution and automated pact identification and installation.

Finally, to evaluate the effectiveness of the security management and risk mitigation efforts at federal agencies, the central office or board could have an "expert review team" at its disposal. This "red team" of 20-25 personnel with the requisite technical skills, could be used to evaluate the cyber security over federal agencies and provide feedback (government-wide) on the "best practices" and common vulnerabilities they encountered.

In fact, I would go so far as to suggest that there ought to be required, by law, an annual test of each agency's vulnerabilities and capabilities (with the latter assessing their ability to respond to events). Further, based on the results of the annual testing process, we could derive baselines that would be applicable across the board, so as to hold all agencies subject to the same standard of account.

(3) **Warning**. A critical step towards coordinating federal agency readiness and preparedness efforts is the construction of a centralized intrusion detection and warning center. Again, the FEDCIRC system could serve as a basis for this system, but would require significant increases in personnel, and budgetary and policy authority. This center would serve a number of critical functions; it would provide indications and warning of an impending attack for all federal agencies; it would employ a federal agency

"infocon" system to establish readiness and preparedness levels on federal agency information systems; it would house a cyber incident response team to assist agencies in incident management; and finally the center could play a crucial role in the implementation of information assurance vulnerability alerts and software patch alerts mentioned previously. This center would serve non-DOD federal agencies, and would work with and parallel the efforts of the Joint Task Force Computer Network Operations that DOD has successfully employed for the past three years.

(4) **Standards**. The federal government needs to improve its standards in both the management of information security systems and the procurement of information technology systems. In the area of security standards management, federal agencies have requirements established in numerous documents including OMB Circular A-130 and several laws. The missing ingredient has been a strict auditing and assessment system to enforce these standards. Specifically, OMB has never been properly manned to implement and enforce such an assessment system. Frequent audits by GAO have demonstrated that, in the absence of a tool to hold them accountable, federal agencies have routinely failed to meet the standards laid out in A-130. If the senior official called for above is given some budgetary review over agencies IT programs, he will have the tool to enforce audit and assessment findings, which would be conducted by the "red team" mentioned above. It would also be beneficial if the results of the audits were provided to the President and Congress as a "report card" to help keep the pressure on federal agencies senior leadership. In the absence of this pressure, many agencies do not treat information security as a critical or core agency mission.

Information technology system procurement standards are another key public sector shortfall. The government needs to have (or work with) a laboratory in which IT products undergo a review and validation process, from which GSA will then provide a list of acceptable products for federal agencies to procure. In the absence of such a procurement standard many federal agencies continue to install information technology equipment with little or no security components installed.

(5) **Training and Education**. There are numerous components of information assurance training and education that the federal government must continue to push.

First, the public sector needs to raise IT security awareness among the general federal workforce. This includes the use of effective security techniques (i.e. passwords) and the need to limit access to IT systems without proper clearance. This awareness training needs to be conducted on a recurring basis, and be tied to an employee's computer access.

Second, we need to continue to train and certify our federal IT security workforce, and to the extent that this mission is out-sourced, ensure that the contractor workforce meets the proper training and certification standards for operating federal systems. Fortunately these training and certification programs are easily available in the private sector, and require very little tailoring for federal government use.

Third, we need to continue to recruit and develop a skilled and "current" IT security management workforce. While IT security managers compose only a small percentage of our federal workforce, these specialists are a rare group of worker and one in great demand in the private sector as well. The Clinton Administration's "Cyber Corps" program was a step in the right direction, identifying and developing university information assurance programs, and recruiting students directly from those few existing programs with scholarships for federal service. An unexpected challenge has been the small number of existing information assurance programs, and the even smaller number of students who were U.S. nationals and thus available for security clearances and federal service. Efforts to develop academic programs, and grow a generation of faculty, need to be closely coordinated between the government, universities, and the private sector, as all three will ultimately benefit from it's success.

From the government's perspective in particular, the aim would be to attract the best and the brightest to public service for at least a portion of their careers. Unless we succeed in doing so, in the long run, our national security will suffer. Put another way, recruitment and retention are, for the public sector, issues as pressing as education and training.

To retain a trained and educated IT security workforce the federal government will have to evaluate its retention and pay packages, for these workers are in heavy demand outside the government as well. We need to introduce reward programs that would not only lay out a promotion path but also establish recognition mechanisms separate from promotion (as was done in Y2K), and we need to revisit the pay scales for these relatively rare but highly prized information security experts.

(6) **Reconstitution**. One area where little headway has been made is the effort to identify public sector information systems, and determine how they will be rapidly reconstituted following a successful cyber attack. This involves not just the federal systems that support our core agency missions, but also the private sector communication and power systems on which the federal systems depend as well. This reconstitution effort raises challenging questions of public – private sector cooperation and coordination that may involve the Defense Production Act and similar legislation. This effort may also identify single points of failure and needed remedies that could have significant budget implications; as such more aggressive attempts to tackle the challenges of reconstitution problem are warranted.

(7) **Research and Development**. The federal government is only a small player in the development of next generation information technology systems. However, in the area of information security systems the work at the DOE Labs and DARPA is still the cutting edge effort. As such, the public sector's R&D efforts are crucial to developing the "next generation" of IT system security, and we must continue to ensure that the DOE and DOD budgets provide a healthy environment for the labs to work in. Additionally, the NSF funds much of the university-based IT research that is looking at the "generation after next" and can therefore impact the consideration of security in those systems.

But the Government is not alone in this endeavor. The private sector is an indispensable partner in protecting critical infrastructures.

The Private Sector: A Crucial New Partner

The benefits from improving the CIPIA readiness of the Private sector are two-fold. First we improve the resilience of our economic infrastructure to cyber attacks and second, we improve our federal government's readiness, because so many critical government functions are conducted on privately owned and operated telecommunication, information and power systems.

Several important steps can be made by the government to support the private sector's CIPIA efforts.

(1) **Encouraging Standards**. Government can – and should – also provide specific incentives to the private sector to better protect its own systems. For instance, government could act as the catalyst for the establishment of industry-wide standards for information assurance in different business sectors, and could establish liability limits against disruption of service for companies using security "best practices." Equally, tax breaks or equivalent "credits" could be accorded to companies that use certified safety products and enforce specific types of security procedures. (The mechanism for certifying the safety and effectiveness of security products should be the consensus product of a private-sector dialogue that government should facilitate).

(2) **Information Sharing**. Government could also grant relief from specific provisions of antitrust laws to companies that share information related specifically to vulnerabilities or threats. Notably, the Freedom of Information Act (FOIA) has been a significant obstacle to public-private information sharing to date because companies run the risk of having sensitive or proprietary data compromised if it is revealed to the public, and fear damage to shareholder confidence if vulnerabilities are publicly acknowledged. Fortunately, FOIA-related obstacles are now being recognized and addressed. Senator Bennett in particular, should be commended for his leadership in this area.

(3) **Liability Relief**. Furthermore, government could provide extraordinary liability relief to the private sector in the case of cyberwarfare (similar to the indemnification authorities set up in the case of destruction of commercial assets through conventional warfare). Financial relief for digital disasters would have insurance companies insuring to a certain level, with government intervening in cases of massive outages or shutdowns. Likewise, a consortium of insurance, software and hardware companies could create a pool for reinsurance purposes.

Although quantifying risk in the cyber area is difficult because of the lack of experience and actuarial data, insurance companies should be encouraged to include in their portfolios limited liability indemnification policies against cyber disruption. Here, government should be the catalyst, not the enforcer, for the creation of parameters and standards.

(4) **Partnering with Federal Government**. In addition to "incentivizing" the private sector in the ways outlined above, government should seek to solidify partnerships

between the public and private sectors. Already, under the auspices of the CIAO, the Partnership for Critical Infrastructure Security has brought together hundreds of leading corporations and various federal agencies to address the problems of infrastructure assurance. This is a good example of a step in the right direction – but we need to do more.

By way of illustration, we should try to improve public-private cooperation through information sharing on: vulnerabilities, warnings of ongoing attacks or threats, hacker modus operandi, and solutions and defenses to established threats and attacks. In doing so, we should try to learn from our experience with the National Infrastructure Protection Center (NIPC), which was not always successfully viewed as the entry point for private sector cooperation with the government. Looking to the future, we should aim to leverage the NIPC's strengths, its ability to conduct complex cyber incident investigations and enforcement. At the end of the day, the NIPC, as an initiative, represents a good start – as a central focus for law enforcement and incident analysis, but not the central point for all forms of private sector cooperation.

Cross-sector cooperation on information sharing is especially important because each sector has its own comparative advantage: whereas government possesses the core insights on CIP from a national security perspective, the private sector possesses the core insights on information security management. With this in mind, government should continue to assist the private sector by interacting constructively with information sharing and analysis centers (ISACs), which are sector-specific associations on the industry side, and by continuing to facilitate cyber security discussions within these various sectors (including banking and finance, telecommunications, and information technology).

Key Issues and Challenges

The suggestions above are not exhaustive, of course. And, even if it were possible to cover the field, it must be conceded that no matter how concerted our efforts are, there will be failures, whether in the public or the private realm. For this reason, reconstitution and business continuity (that is, the restoration of essential systems and services) is a matter that we cannot afford to ignore. Indeed, continuity of operations and government may be the key to deterrence: if we can restore our systems and provide business continuity in relatively short order following an attack, the incentive to engage in further attacks of the same sort in future should be diminished. Now more than ever, the public and private sectors need to work together to ensure our nation's continued health and vitality. The private sector needs to appreciate its role in protecting our nation and visa versa.

The Internet truly became an invaluable tool during and after the 11 September terrorist attacks. It proved a valuable tool for the government to disseminate vital information and for businesses to continue functioning. FirstGov.gov fashioned a special section to provide information to the public in the form of links to relief services, status updates, and federal and private organizations providing public response and recovery services. The FBI established channels to receive information regarding their investigations on the Internet. The Internet did what it was designed to do – facilitate communication – and in so doing clearly demonstrated its significance. In the midst of the physical turmoil, the virtual world continued to function. However, there may be a dark side.

Stories abound about al Qaeda's use of the Internet – the full extent of which is not yet known. Reports claim their cyber tradecraft ranged from the highly sophisticated, like steganography, to the comparatively innocuous, like code words or phrases. An email reminding someone to "walk the dog" could have been a covert signal to proceed with an attack. No amount of computing power or code breaking could have tumbled that clue. We do know that in the past their techniques have involved a combination of both high-tech and low-tech means of tradecraft and communication.

Our policies in response to threats of any kind, moreover, must not stifle the engines of innovation that drive our economy and enhance our lives. Unfortunately, we have been trying to prosecute 21st century crimes armed only with 19th century laws. This must change and I applaud Congress efforts to empower our federal agencies with the needed statutory authorities.

Now more than ever, we cannot afford to overreact or put up too many virtual or physical walls or the bad guys win by default because we have lost our way of life. The cure must never be worse than the disease – undoubtedly the benefits outweigh the risks.

In particular, some seem to think that privacy, security and electronic commerce are mutually exclusive. This is just not so. The "game" is not zero-sum: we can – and should – ensure privacy, security <u>and</u> e-commerce. Indeed, it would be fair to state that you cannot have privacy without security, and without security, e-commerce will never flourish.

At the end of the day, it all comes down to leadership –not only in government, but in the private sector and on the part of individuals, too. President Bush, and his team, deserves much credit for piloting the ship of state through these roiling waters. America rests easier knowing that he is at the helm and is charting our course. And we are grateful to the other world leaders who stand with us. But make no mistake, we are in the eye of the storm. Fighting terrorism will take not only new strategies and new tools, but also the old grit and determination that have been America's historical reactions to unjust aggression and war.

In political terms, some of the difficult battles are still to come. Combating terrorism – in all its forms – requires a sustained campaign. This campaign will continue to demand united support for years. While I hope that the intense focus of the spotlight shifts away from the issue soon, I urge Congress to continue its unified efforts on this front.

That said, while the president and Congress have already demonstrated political will on this matter – and I say this will all sincerity – that alone will not be enough. We all share responsibility for this issue and we must all muster the will, and be prepared to contribute the resources, to deal with it. Plainly, the challenges that we face are great. But we, as a nation, are up to the task.

CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE?

Testimony of
Kenneth C. Watson
President, Partnership for Critical Infrastructure Security

To

US Senate
Committee on Governmental Affairs

October 4, 2001

Good morning Chairman Lieberman, Senator Thompson, and distinguished Committee Members. I am honored to be here today on behalf of the more than 70 companies and organizations that comprise the Partnership for Critical Infrastructure Security, or PCIS. The question you are asking, "Critical infrastructure protection: who's in charge?" appears aimed at discovering leadership. America would like to be able to turn to a single government executive or agency, and perhaps one industry belly button, with the authority and responsibility to assure the continued delivery of vital services to our citizens in the face of new and emerging threats. What you will actually discover is an architecture that requires distributed leadership, cooperation, and *partnership* to accomplish that goal.

The need to coordinate and manage the assurance of our nation's critical infrastructures is not something industry and government just started considering since September 11. The members of the Partnership and our government counterparts have been working on this since 1999, and some industries, such as the telecommunications sector, have had formal working relationships with government agencies dating from the early 1980s. I'd like to describe for you the environment of the critical infrastructures, explain what we were doing before the horrendous attacks three weeks ago, and what has changed since then. I'll also have recommendations for the Congress and the American people.

The Architecture

Over the last 10 to 20 years, the United States, and the rest of the developed world, have truly changed the way we live and work, and there is no turning the clock back. Each industry is now dependent on every other, and we are all dependent on computer networks. The Federal Government cannot function without services provided by private-sector infrastructure owners and operators. Many of these are multinational corporations, and all have an interlaced network of suppliers, partners, and customers. The Internet itself relies on key nameservers and routers located around the world, with no central ownership or authority. The health of the global economy is directly relevant to the health of America's national and economic security.

Just as the Internet is open, borderless, international, and unregulated, responsibility for protecting critical infrastructures is distributed among companies and government organizations. Distribution of control is actually safer than centralization, and builds resilience into the architecture. Form follows function. This applies not only to architecture, but also to how we organize to protect our critical infrastructures.

Even with the best of intentions and the most modern tools, the Defense Department could not defend America against a cyber attack on a power plant in Omaha, that happens to provide power to a major railroad hub's switching center. Critical infrastructure protection requires a true public-private partnership, with all the trust that implies, to succeed. Activities that an enterprise can take—conducting vulnerability and risk assessments, deploying security technologies, investing in research and development, creating incident response teams—must now be distributed and coordinated. Many in industry and government have been focusing on exactly how to accomplish this coordination for at least the last five years.

Partnerships

The President's National Security Telecommunications Advisory Committee, or NSTAC, was established in 1982 to provide advice on national security and emergency preparedness issues in the telecommunications sector. Comprised of most key service and equipment providers, the NSTAC has consistently discovered and made recommendations to mediate problems in that critical infrastructure.

The President's Commission on Critical Infrastructure Protection, reporting in October 1997, recognized that the need to coordinate closely between the public and private sectors for economic and national security no longer applied to a single infrastructure sector. The Marsh Commission correctly identified the vulnerability of all our infrastructures to errors and intentional attacks, their interdependency in both the cyber and physical dimensions, the dependence of government on private-sector infrastructures, and the resulting requirement for a robust public-private partnership to develop solutions. Industry responded to the government invitation to a dialog by launching the Partnership for Critical Infrastructure Security at the World Trade Center on December 8, 1999.

Since its formation, the PCIS has become a model for cross-sector coordination, public-private cooperation, and a clearinghouse for timely information needed by critical stakeholders. Last year, the PCIS identified barriers to information sharing with government, and now the Congress is working through legislation based on our findings. During the response to the Code Red worm, the PCIS represented industry alongside the FBI and security experts as we made the public service announcement that ultimately blunted the impact of that infestation. Later this year, the government will publish the unique public-private National Plan, with industry sections coordinated by the PCIS.

I mentioned before that this is not just an American problem. Several countries are following our example, establishing similar partnerships. The PCIS is forming close relationships with them, and we plan to collaborate in several key areas. Earlier this year, Canada established the Office of Critical Infrastructure Protection and Emergency Preparedness, and its head, Margaret Purdy, has attended several PCIS meetings. We are using the results of Canada's outstanding interdependency vulnerability study as we look at our own. The United Kingdom recently formed the Infrastructure Assurance Advisory Council, and its Executive Director, Dr. Andrew Rathmell, will be speaking at the next PCIS Board meeting later this month. Switzerland's Infosurance program is a public-private infrastructure security partnership very similar to ours. In August this year, the United States and Australia held a bilateral meeting in Canberra, where we agreed to collaborate on several key initiatives, including international security standards.

There are several other public-private and international partnerships: the Forum for Incident Response and Security Teams, or FIRST; the Worldwide Information Technology Security Association; and others, mainly in the information technology sector. Many people and organizations are beginning to grasp the significance of the distributed nature of the new economy, its implications on economic and national security, and the absolute requirement for partnership and collaboration.

Information Sharing

One of the keys to success is effective and timely information sharing about threats, vulnerabilities, countermeasures, and best practices within and between industries, and between the public and private sectors. Information Sharing and Analysis Centers, or ISACs, are proving their value as both computer defense centers and awareness vehicles. There are currently five ISACs in operation:

- Financial Services
- Telecommunications
- Information Technology
- Electric Power
- Oil and Natural Gas

These ISACs have shared information on threats to members and helped their sectors prevent damage and disruption from threats like Code Red, Nimda, and Vote. The Telecom ISAC, with its connections to National Infrastructure Protection Center (NIPC), Joint Task Force –Computer Network Operations (JTF-CNO), FedCIRC, and National Communications Systems (NCS), is able to share vital information from the government to industry that has proved both valuable and timely.

Four additional ISACs are in various stages of development:

- Railroads
- Aviation
- Water
- Information Service Providers

One of this year's top goals for the PCIS is to establish a cross-sector and public-private information-sharing architecture. The existing ISACs, under the leadership of the NCS, met on September 26, 2001 to develop operational information-sharing capabilities. This meeting greatly accelerated the progress we have made in this area, and the procedures they develop will form the foundation for the overall PCIS cross-sector architecture. They agreed to the following steps:

1. ISAC operational elements will immediately exchange e-mail, telephone numbers, and operational interfaces.

2. ISACs will pass traffic deemed appropriate to other sectors that does not duplicate publicly available information, but addresses concerns to both physical and cyber elements of sector infrastructures.

3. The Telecom ISAC will draft an SOP in one week (due yesterday), using operating rules from all the ISACs.
4. The Telecom ISAC will provide a phone bridge that any ISAC can use to initiate an alert to all.
5. NCS will offer a port to any ISAC operations center wishing to join the ACN
6. as a second tier of communications.
7. The ISACS will establish this pilot program for 60-90 days and then assess expanded participation.
8. NCS provided GETS cards to ISAC operations centers.
9. The Telecom ISAC will share government information as widely as possible with all ISACs.

What changed on September 11?

Information technology took a huge hit on September 11. In addition to the people that we can never replace, one estimate places losses in IT resources by the financial community alone at $3.2 billion.

- Verizon's switching office at 140 West St. in Manhattan, supporting 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites.
- AT&T lost fiber optic equipment in the World Trade Center and had switching equipment damaged in a nearby building. Remarkably, AT&T switching gear in the basement of the World Trade Center continued to function.
- Sprint PCS wireless network in New York City lost four cells.
- Cingular Wireless lost six Manhattan cell sites.
- Worldcom lost service on 200 high-speed circuits in the World Trade Center basement

But like the United States, the Internet was created as an open society, with multiple communications paths and built-in resilience. Because of its redundancy, the Internet provided many of the needed paths for communication immediately following the attacks in New York and Washington.

The day of the attack:

- AOL Instant Messenger logged 1.2 billion messages – 100 times usual message volumes.
- Verizon and AT&T reported that call volume and long-distance traffic doubled

One week after the attack, Verizon announced that it had restored 1.4 million of 3.5 million data circuits, and the New York Stock Exchange had phone and data service to 14,000 of its 15,000 lines. The exchange handled 2.37 billion transactions without incident on its first day back in operation.

Other infrastructures also demonstrated tremendous robustness and cooperation. Diesel generators were brought in to provide power for lighting, telecommunications, and Internet access in lower Manhattan. All the involved sectors and governments worked together, overcame a restriction on diesel fuel deliveries, and accomplished the miracles we have all witnessed.

The terrorist attacks on the World Trade Center and the Pentagon did not change the architecture of the new economy, our interdependency, or the interlinked nature of the economies and national security of the nations of the develop world. What those attacks did was to create a sense of urgency and a need to "do something" about security among those that had paid little attention to security before. Just as the Administration carefully and deliberately seeks out those that conducted and supported these barbaric acts and learns about this new battlefield environment, I urge the Congress, the Administration, and the American people not to move too quickly to try to solve the infrastructure protection problem.

The challenge for this Administration is to streamline its organization to become an effective partner to industry. The current mix of lead agencies, sector liaisons, and uncoordinated budgets makes synchronized action difficult. The Critical Infrastructure Assurance Office (CIAO), working with the National Coordinator for Security, Critical Infrastructure Protection, and Counter-Terrorism, has overcome immense obstacles and achieved a high level of cooperation and coordination among government departments and agencies.

We believe the events of September 11 will also ultimately result in changes to the National Plan for Critical Infrastructure Protection, for which the PCIS plays a key coordination role. We will work closely with the CIAO as the government organizes itself to manage Homeland Security, Counter-Terrorism, and Critical Infrastructure Protection. We are confident that there will be much more on cross-sector reconstitution in the plan than originally envisioned.

Recommendations

So what can we do to protect our critical infrastructures? We can raise the bar of security worldwide, through research and development, interdependency vulnerability studies, information sharing, raising awareness, and removing legislative barriers.

1. Support Administration initiatives to streamline coordination within the Federal Government. Any overall federal coordinator must have budget authority and accountability to be effective.
2. Support initiatives that will secure the next-generation network of networks as well as the patches and fixes we are applying today. The PCIS is developing a research and development road map that will include a gap analysis of current industry, academic, and government programs, and recommendations for focusing resources to meet sector and cross-sector needs.
3. Encourage government organizations, businesses, and individuals to practice sound information security. Several organizations publish lists of effective means to secure computers and networks against malicious activity, like updating passwords, disallowing unauthorized accounts and unneeded services, and installing firewalls and intrusion detection. This is now not just common sense, it is a matter of cyber civil defense.
4. Carefully consider the impact of any new legislation on the freedoms Americans cherish—individual privacy, freedom of expression, and entrepreneurship. We all understand that without security there is no privacy, but we must always strive for balance.

The PCIS Public Policy Working Group is investigating many areas of current and pending legislation with the purpose of discovering ways to improve critical infrastructure assurance at all levels. We welcome any invitation to discuss our activities with you at any time. We believe a dialog where we can hear your insight, and you can hear our concerns, will be healthy and fruitful.

We are all in this together—industry, academia, the Administration, the Congress, and the American people—and we need all points of view to ensure that our critical infrastructures continue to provide for the health and welfare of all citizens and the pursuit of liberty.

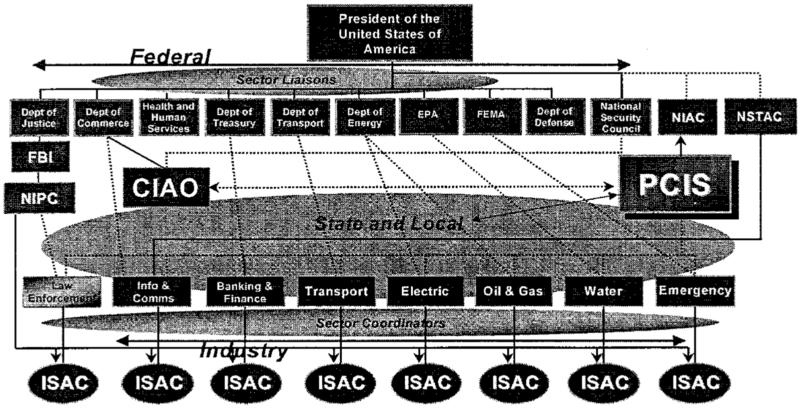
Thank you very much. I'm happy to answer any questions you have.

PCIS Board of Directors

Association of American Railroads	Ed Hamberger, President
Association of Metropolitan Water Agencies	Diane VanDe Hei, Executive Director
Bank of America	Rhonda MacLean, Chief Information Security and Business Continuity Officer
BellSouth Corp.	Bob Wright, Director, Information Security
Cisco Systems, Inc.	Ken Watson, Manager, Critical Infrastructure Assurance Group
Consolidated Edison Company of NY	Lou Rana, Vice-President
Information Technology Association of America	Harris Miller, President
The Institute of Internal Auditors	Bill Bishop, President
Merrill Lynch & Co., Inc. Officer	Steve Katz, Chief Security and Privacy
Microsoft Corporation	Howard Schmidt, Chief Security Officer
Conoco, Inc.	Billy Gillham, Manager, Global Security
North American Electric Reliability Council	Michehl Gent, President
Telecommunications Industry Association	Gerry Rosenblatt, Director, Technical and Regulatory Affairs
Union Pacific Corporation	Rick Holmes, Director, Information Technology
United States Telecom Association	Fred Tompkins, Director, Network Assurance

PCIS Relationships

Relationships



President of the United States of America

Federal

Sector Liaisons

Dept of Justice

Dept of Commerce

Health and Human Services

Dept of Treasury

Dept of Transport

Dept of Energy

EPA

FEMA

Dept of Defense

National Security Council

NIAC

NSTAC

FBI

NIPC

CIAO

PCIS

State and Local

Law Enforcement

Info & Comms

Banking & Finance

Transport

Electric

Oil & Gas

Water

Emergency

Sector Coordinators

Industry

ISAC

ISAC

ISAC

ISAC

ISAC

ISAC

ISAC

ISAC