[Senate Hearing 106-858]
[From the U.S. Government Publishing Office]

S. Hrg. 106-858

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: THE THREAT IS REAL

==========

HEARING

before the

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,
AND GOVERNMENT INFORMATION

of the

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

on

EXAMINING THE PROTECTION EFFORTS BEING MADE AGAINST FOREIGN-BASED THREATS TO UNITED STATES CRITICAL COMPUTER INFRASTRUCTURE

_____

OCTOBER 6, 1999

_____

Serial No. J-106-53

_____

Printed for the use of the Committee on the Judiciary

_____

U.S. GOVERNMENT PRINTING OFFICE
68-563 WASHINGTON : 2001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, Chairman

STROM THURMOND, South Carolina	PATRICK J. LEAHY, Vermont
CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
ARLEN SPECTER, Pennsylvania	JOSEPH R. BIDEN, Jr., Delaware
JON KYL, Arizona	HERBERT KOHL, Wisconsin
MIKE DeWINE, Ohio	DIANNE FEINSTEIN, California
JOHN ASHCROFT, Missouri	RUSSELL D. FEINGOLD, Wisconsin
SPENCER ABRAHAM, Michigan	ROBERT G. TORRICELLI, New Jersey
JEFF SESSIONS, Alabama	CHARLES E. SCHUMER, New York
BOB SMITH, New Hampshire	

Manus Cooney, Chief Counsel and Staff Director

Bruce A. Cohen, Minority Chief Counsel

_____

Subcommittee on Technology, Terrorism, and Government Information

JON KYL, Arizona, Chairman

ORRIN G. HATCH, Utah	DIANNE FEINSTEIN, California
CHARLES E. GRASSLEY, Iowa	JOSEPH R. BIDEN, Jr., Delaware
MIKE DeWINE, Ohio	HERBERT KOHL, Wisconsin

Stephen Higgins, Chief Counsel and Staff Director

Neil Quinter, Minority Chief Counsel and Staff Director

C O N T E N T S

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: THE THREAT IS REAL

WEDNESDAY, OCTOBER 6, 1999

U.S. Senate,
Subcommittee on Technology, Terrorism,
and Government Information,
Committee on the Judiciary,
Washington, DC.

The committee met, pursuant to notice, at 10:01 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Jon Kyl (chairman of the subcommittee) presiding.
Also present: Senators Feinstein, and Bennett (ex officio).

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator Kyl. The hearing before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information will please come to order.
Today's hearing is on the subject of the critical information infrastructure and protection of the infrastructure and the threat thereto. Our panelists this morning, we will have two panels, and on the first panel, we have Mr. John S. Tritak, who is Director of the Critical Information Assurance Office in Washington, and Mr. Michael Vatis, the Director of the National Infrastructure Protection Center here. The second

panel will be Mr. Jack Brock, Director of Information Management Issues at the General Accounting Office. I appreciate the attendance of the witnesses here.

I am informed that other members of the subcommittee will be arriving, but in view of the schedules of everyone concerned, I am going to begin the hearing right on time and we will move forward from there.

Let me first of all make a brief opening statement and then call upon our two witnesses to make an opening statement, after which we will have a series of questions.

At our hearing today, we are going to examine a growing public policy concern, the threat of hostile attack on our Nation's critical information infrastructure and the adequacy of the Federal Government's response to this threat. This is the fourth public hearing that our subcommittee has held on the topic in the last 2 years, and given the importance of the subject, it will not be our last.

The President's top advisors recently issued a report on preserving America's privacy and security in cyberspace. As the report points out, the enormous success the United States has enjoyed over the past century was due in part to the ability of our Nation and its leaders to deal with the latest technological trends in a way that enhanced the security and prosperity of successive generations of Americans. At critical junctures in our history, wise government policies with regard to innovative technology have resulted in unprecedented success.

During the industrial age, the arrival of World War II signaled an urgent need for increased production and scientific advances. The success of America's war effort in defeating fascism rested largely on the strength of our industrial might and the successful collaboration between our government and industry. We not only protected America's security, but also vaulted the U.S. economy to unprecedented heights in the post-war period.

Today, the industrial age has become the information age and computers facilitate the instant exchange of vast amounts of data and ideas. Who would have predicted just a few decades ago that a small Defense Department research effort would result in the creation of the Internet and revolutionize our society.

As we approach the dawn of the new millennium, America again faces a time of pivotal change. Information technology presents both an opportunity and a threat to our society, which is increasingly dependent upon computers and communications equipment, what we call our critical information infrastructure. As most Americans have learned recently, with the preparations for Y2K to make sure there are no major disruptions in services, virtually every key service is dependent upon computers, from electric power grids, to phone systems, to air traffic control, water and sewer service, medical devices, banking, and the list goes on and on. Unfortunately, very few of these critical computer networks were designed with good security measures.

The changes in our society also must be viewed in context with America's changing geopolitical role in the post-Cold War world. The United States is the world's only superpower and our armed forces enjoy technological superiority on the battlefield. Nations and terrorist groups that are hostile to our interests are increasingly choosing not to confront our strengths directly, that is, by trying to field fleets of advanced fighter planes or ships on par with ours, but rather are seeking to exploit our vulnerabilities, looking hard for an Achilles heel.

According to the National Security Agency, over 100 countries are working on information warfare techniques. One recent case illustrates the danger of this threat. According to Newsweek magazine, computer systems at the Defense and Energy Departments have been the subject of a sustained computer hacking effort from Russia. These attacks have resulted in the loss of vast quantities of data, possibly including classified naval codes and information on missile guidance systems.

These computer attacks have reportedly been very subtle. For example, the London Sunday Times interviewed an engineer at the Space and Naval Warfare Systems Command in San Diego, CA, who described being alerted to a problem when a computer print job took an unusually long time. According to the Times, ``To his amazement, monitoring tools showed that the file had been removed from the printing queue and transmitted to an Internet server in Moscow before being sent back to San Diego.''

And there are other troubling examples of computer attacks by U.S. citizens that demonstrate our weaknesses in this area. For example, one group dubbed the ``Phonemasters'' by the FBI manipulated computers that route telephone calls. These hackers reportedly gained access to telephone networks of companies like AT&T, British Telecom, GTE, Sprint, MCI WorldCom, and Southwestern Bell.

At times, these hackers were able to eavesdrop on phone calls, compromise databases, and redirect communications at will, according to press accounts. In addition, they apparently had access to portions of the nation's power grid and air traffic control systems and hacked their way into a digital cache of unpublished phone numbers at the White House. In one prank, this group even succeeded in forwarding FBI phone lines to sex-chat lines in Germany, Moldavia, and Hong Kong, resulting in the FBI being billed $200,000 for these calls.

These calls would be amusing if the stakes were not so high. Given a more malicious intent, hackers in our country, or those working for terrorist groups of the military services of nations hostile to the United States, could do far greater damage to our critical information infrastructure, resulting in what some have termed ``an electronic Pearl Harbor.'' We have been fortunate that the United States has escaped serious harm thus far, but our luck is likely to run out unless we take aggressive steps to tighten these gaps. As Winston Churchill once observed, in history, ``the terrible `ifs' accumulate.''

At today's hearing, we will explore how our government has approached this problem as well as how its efforts might be

improved. We will also discuss whether new legislation is required and we will explore the impact of the government's cyber-protection efforts on the privacy of American citizens.

Our witnesses are ideally suited to address these issues. Mr. John Tritak, Director of the Critical Information Assurance Office, is responsible for the development of an integrated national plan to address the threats to our critical infrastructure. He will be followed by Michael Vatis, the Director of the National Infrastructure Protection Center, an interagency organization that is charged with leading the Federal Government's efforts to detect, prevent, investigate, and respond to cyber attacks on U.S. critical infrastructures.

And on our second and final panel, Mr. Jack Brock, Director of Government Information Systems at the GAO, will testify about the type of vulnerabilities to cyber attacks that exist in computer networks operated by Federal agencies that the GAO has identified during annual audits and the status and effectiveness of the government's effort to reduce these vulnerabilities.

It is my great pleasure to turn first to Senator Dianne Feinstein of California and then to Robert Bennett of Utah, two of the real experts in the U.S. Senate on this subject. Senator Feinstein is the ranking member of this subcommittee. She and I have been working for a long time, concerned about the protection, the necessity of protecting our Nation's critical infrastructure.

Senator Bennett, not even a member of this committee, has such an interest in this subject that as chairman of the special Y2K Committee here in the Senate, he has taken an interest in what we are doing and what others in the Congress are doing to deal with this issue. It is largely to his credit, through the Y2K Committee chairmanship, that a lot of this information has been brought to light to the American public at large. So I am really pleased that Senator Bennett is here with us, as well.

Senator Feinstein.

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator Feinstein. Thanks very much, Mr. Chairman. I think you know how much I enjoy working with you and I want to thank you for your leadership on this subject. I think I probably do not qualify as an expert. I think my colleague, Senator Bennett, probably does. But I think I do qualify as someone that believes that this area is one of the most critical and crucial areas we now face, how to address the serious and increasing threats to our national infrastructure.

The advent of a new technology age in which we now live has brought America certainly great prosperity. California, my State, has benefitted immensely from these developments. Powerful computers now control our electricity, our phone service, our plane traffic, our national defense, and they have moved us forward much more quickly than anyone ever could have

imagined. We can plan our physical infrastructure more efficiently. We can test prototype aircraft on a computer screen without ever spending a dime on construction. We can allocate resources more efficiently and at a lower cost than ever before.

And the power of a new global communication network has taken people from the ends of the earth and brought them together, almost as if they were next-door neighbors. Amazing. Ten years ago, sending a message through the mail from Cairo to California would take weeks. Now, that simple message can be sent with a simple stroke of a key and accomplished in the blink of an eye. That power, the power of instant, inexpensive communication across mountains, oceans, and international boundaries has opened up vast potential for global cooperation and a truly borderless economy.

But, and here is the but, with that power, also comes extraordinary danger. Just like an e-mail from friend to friend can travel over the ocean and across national boundaries in a split second, so can a computer virus or a casual hacker attack or a foreign cyber terrorist. As a result, this Nation faces serious challenges in the coming months and years. We must learn to balance the benefits of global interconnectivity with the need to protect our vital information, our defense, our infrastructure.

About a dozen countries have information warfare programs. They include Libya, Iraq, and Iran. Foreign intelligence services routinely break into American public and private sector computers, mapping power grids to find weak links and leaving trap doors at virtually every U.S. military base.

Last year, two California high school sophomores were among a group suspected of penetrating and compromising at least 11 sensitive computer systems and military installations and dozens of systems at other government facilities, including Federal laboratories that perform nuclear weapons research. These children were just looking for some excitement, and guess what, they found it. But imagine if they had been out to do real damage. Imagine if they had been employed by a hostile foreign government.

Because of the interrelated nature of our critical infrastructure systems, today's terrorist has the potential to do with a keyboard what in the last world war might have taken a squadron of bombers to accomplish. At stake are not only the information systems upon which we rely, but the electric power grid, the public switch communications network, the air traffic control system, the banking system, rail transport, oil and gas distribution networks, and a host of other networks on which our national security and our way of life today depend.

We have begun to address this threat. Presidential Decision Directive 63, issued last year, identifies critical infrastructure protection as a national security priority and commits us to effectively protect our critical infrastructures within 5 years. But the time table established by Public Directive 63 is already slipping. A national report was due to Congress last December. As of today, we have still not seen it.

I look forward to examining today what our government has done to protect our critical infrastructure and what more can be done. This Congress and this subcommittee has a clear responsibility to do what it takes to protect this Nation from the threat of cyber terrorism and from the enormous risks that come hand in hand with the advances in technology that have given us so much over the last few years.

So thank you, Mr. Chairman, for your leadership and for scheduling this hearing and your very serious attention to this issue.

Senator Kyl. Thank you for a fine statement, Senator Feinstein.

Now, I would like to turn to Senator Robert Bennett for any comments he may have.

STATEMENT OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM THE STATE OF UTAH

Senator Bennett. Thank you, Mr. Chairman. I appreciate your courtesy in allowing me to come where non-lawyers usually do not appear. I understand Senator Feinstein is not a lawyer, and that----

Senator Feinstein. I am not a lawyer.

Senator Kyl. Now, you guys quit bragging. [Laughter.]

Senator Bennett. That demonstrates how open-minded you are on this committee.

I think you are having the first of what will be a long series of hearings. This is an issue which we are only barely beginning to understand, but I think, ultimately, the next President, whomever he or she may be, will find that the challenge of information warfare will be the number one national security issue of the next administration.

I recently went to an office where they had drawn a map of the new world. Whenever you think of military threats, you start out with the geography and you draw the map and the various sides. This was a map of the Internet and it did not look like any map you or I have ever seen before. It looked like an abstract painting. I wanted to take it down and put it in my office.

The world geologically is billions of years old. The world electronically is 10 years old or less. And the one thing that was striking about this map is that there were no oceans on it. When we talk about the U.S. militarily, we talk about the sanctuary of North America between two oceans, and on this new map of the new world, there were no oceans and no sanctuary. Mr. Chairman, you and Senator Feinstein have summarized this very well in your statements.

The reason I think this hearing is important is because we do not have in our present governmental structure a neat pigeon hole in which to put this particular threat. For example, if somebody does the kinds of things that Senator Feinstein was describing, is that a military attack on our national security and, therefore, the responsibility of the Defense Department, or is that a violation of private property rights and,

therefore, an issue for law enforcement, or does it become both? And where do the responsibilities lie for the Defense Department to protect us from foreign attack and from the Justice Department to protect us from intrusions?

Inevitably, in this new world, those intrusions will merge. Foreign efforts to destroy us, cripple us, do us harm, will very clearly merge with domestic capabilities to break in. We have already seen the example of a foreign agent who hired some American teenage hackers, and as Senator Feinstein said, they were out for the thrills and experience, but their mentor had a much more malicious purpose in mind.

I think the Judiciary Committee is the logical place to be holding these kinds of hearings. I have talked with Senator Roberts, who plans to be holding hearings in the Armed Services Committee, and we, of course, have held some hearings on this in the Senate Special Committee on the Year 2000. Some of your witnesses here today have already testified before that committee.

So, as I say, I think this is the first of what will be a series of hearings. Ultimately, I think the issue must come before the Senate leadership and the House leadership to say where appropriately within the legislative structure does the responsibility lie for oversight and coordination of this very, very important challenge.

So I congratulate you on your hearings and I am very grateful for your willingness to allow me to participate.

Senator Kyl. Thank you very much, Senator Bennett.

Now to our panel. Mr. John Tritak, you will lead off, and then Michael Vatis.

PANEL CONSISTING OF JOHN S. TRITAK, DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, WASHINGTON, DC; AND MICHAEL A. VATIS, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, WASHINGTON, DC

STATEMENT OF JOHN S. TRITAK

Mr. Tritak. Thank you, Senator Kyl, Senator Feinstein, Senator Bennett. It is truly an honor to be here today to discuss the challenges facing our Nation in the area of critical infrastructure protection and the efforts being undertaken by the administration to address those challenges. I intend to keep my opening remarks very brief and ask that my written statement be entered into the record.

Senator Kyl. All of the statements will be admitted, without objection.

Mr. Tritak. Thank you, sir. America has long relied on complex systems or critical infrastructures to assure the delivery of services vital to its national security, economic prosperity, and social well-being. These infrastructures include telecommunications, electric power, oil and gas delivery and storage, banking and finance, transportation, and vital human services and government services. The information age has fundamentally altered the nature and extent of our

reliance on these infrastructures.

Our government, our economy, our society, indeed, our individual lives are becoming increasingly dependent on an ever-expanding system of networks of computers and information systems. The increasing dependence on computer control networks, combined with the growing interdependence of our Nation's critical infrastructures, together present a new kind of vulnerability, especially to deliberate attack.

The threats posed to our critical infrastructures are real and growing. The nature of these threats and the potential risks they pose to the Nation's infrastructures will be addressed by Mr. Vatis of the National Infrastructure Protection Center.

PDD 63 was issued in May 1998 to take up the unique challenges posed by these threats. I say unique because the risks posed to our critical infrastructures present a challenge that is really unique in our history, as this may very well be the first time a national security challenge cannot be solved by the government alone. Indeed, 90 percent of the infrastructures that we are concerned about are privately owned and operated.

This is why PDD 63 stresses the importance of establishing public-private partnerships and why the President has designated lead agencies in the Federal Government to work as liaisons with the respective sectors to build those partnerships. PDD 63 also recognizes the traditional areas of national defense, foreign affairs, intelligence, and law enforcement and that they are fundamental to protection of our infrastructures, inherent in the domain of government, and stipulates that sector coordinators be designated for these areas from the associated government agencies.

Shortly, the administration will publish the first version of a plan to implement PDD 63. The draft is in the final stages of interagency clearance, so I cannot go into a great deal of detail on its content. However, I can highlight the themes that are captured in the plan as well as what is contained in PDD 63.

First is a continuing commitment to protecting those infrastructures that are necessary in order to perform national defense and intelligence missions. I believe you have submitted for the record the statement by Mr. Richard Schaeffer of the Office of the Secretary of Defense, who lays out in great detail what efforts are being undertaken in that regard to protect those infrastructures.

Second is a need for the U.S. Government to serve as a model in critical infrastructure protection. Recognizing that maybe most of the critical infrastructures of our country are privately owned, it is very difficult for the government to call upon private industry to take up the challenge posed by PDD 63 unless it has its own house in order. With that in mind, the President charges the Federal Government to do what it needs to do to ensure that its critical infrastructures are protected against intentional attack.

Third and finally, there is a need to establish the

partnerships between private industry and the government on the one hand and to encourage information sharing arrangements first and foremost within industries themselves and ultimately between industry and government. Those partnerships at various levels, we believe, will secure our Nation's infrastructures over the long term and that a collaborative effort will ensure that creative solutions are developed to meeting the challenges of the future.

I would like to conclude my remarks very briefly by highlighting some of the key programs that are likely to appear in a national plan, as they are deemed sufficiently important by the administration to request accelerated funding in the fiscal year 1999 budget amendment, which is before you at the moment.

The first of these supports an aggressive government-wide implementation of a Federal computer security requirements program. The proposal requests $5 million to establish a permanent 15-member expert review team that would assist government agencies in identifying vulnerabilities, plan secure systems, and to implement critical infrastructure protection plans. The Critical Infrastructure Assurance Office under PDD 63 is to assist agencies in identifying critical systems and their own dependencies, and we will be working and supporting the expert review team in that effort.

Second, the administration requests $8.4 million to establish a Federal intrusion detection monitoring system to secure Federal Government computer systems. A couple of key points I would like to make about that briefly, given the amount of coverage that has been given to this issue in the press.

First, this is meant to cover civilian government agencies only. This is not meant to be wired into the private sector or to include private industries in some fraud monitoring system.

It provides a centralized capability to analyze anomalous activities that agencies may detect through the use of their monitoring systems.

Fourth, any Federal intrusion detection monitoring system that is developed will be fully consistent with existing privacy laws. No additional authorization has been given to the government in order to implement this program.

Finally, in cases where activity suggests criminal intent and criminal activity, those and only those pieces of information will be going to law enforcement, as appropriate under existing laws.

The third request is for approximately $17 million for the recruitment, training, and retention of Federal information technology managers and officers. The purpose of this program is to ensure that the Federal Government, if it is to act as a model, has the capabilities to protect its information infrastructures against malicious intent and activity.

Four, $7 million are requested for ongoing efforts to secure government-to-government communications through the establishment of public key infrastructures.

Fifth and finally, $2 million is being requested to support

two pilot programs to foster information sharing arrangements between State and local governments and private industry.

I would like to thank you for having me here today and I welcome any questions you may have.

Senator Kyl. Thank you very much.

[The prepared statement of Mr. Tritak follows:]

PREPARED STATEMENT OF JOHN S. TRITAK

Mr. Chairman, Madame Ranking Member, members of the Subcommittee, ladies and gentlemen, it is an honor to appear before you here today to discuss the challenges facing our Nation in the area of critical infrastructure protection. This Subcommittee has shown exceptional leadership on these issues, and I am grateful for the opportunity to work closely with you and the Congress to find ways to advance infrastructure assurance for all Americans. We all recognize that no viable solutions will be discovered or implemented without the executive and legislative branches working together for our national good.

I. INTRODUCTION

America has long depended on a complex of systems--or critical infrastructures--to assure the delivery of services vital to its national defense, economic prosperity, and social well-being. These infrastructures include telecommunications, electric power, oil and gas delivery and storage, banking and finance, transportation, and vital human and government services.

The information age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our government, economy and society are being connected together into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence comes new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in. the world can potentially break into sensitive government files, shut down an airport's air traffic control system, or cause a power outage in an entire region.

The threats posed to our critical infrastructures by hackers, terrorists, criminal organizations and foreign governments are real and growing. The nature of these threats will be addressed by Mr. Vatis of the National Infrastructure Protection Center (NIPC).

Before I discuss the initiatives the Administration is undertaking to secure our nation's critical infrastructures, I would like to discuss the historical context within which PDD-63 arose.

In the early 1990's, events such as the 1995 bombing of the Murrah Federal Building in Oklahoma City demonstrated that the federal government needed to address new types of threats and vulnerabilities--many of which the nation was unprepared to defend against.

In response to this tragedy, and other events, the Administration formed an inter-agency working group to examine the nature of the threat, our vulnerabilities, and possible long-term solutions for this aspect of our national security. The Critical Infrastructure Working Group (CIWG), chaired by then Deputy Attorney General Jamie Gorelick, and including representatives from the Defense, Intelligence, and

national security communities, identified both physical and cyber threats and recommended formation of a Presidential Commission to address more thoroughly many of these growing concerns.

In July 1996, in response to the CIWG recommendation, President Clinton signed Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP or, the Commission). After examining infrastructure issues for over a year, the Commission issued its report, Critical Foundations, Protecting America's Infrastructures, drawing at least four significant conclusions:

First, critical infrastructure protection is central to our national defense, including national security and national economic power;

Second, growing complexity and interdependence between critical infrastructures may create increased possibility that rather minor and routine disturbances can cascade into national security emergencies;

Third, vulnerabilities are increasing steadily and the means to exploit weaknesses are readily available; practical measures and mechanisms, the commission argued, must be urgently undertaken before we are confronted with a national crisis; and

Fourth, laying a foundation for security will depend on new forms of cooperation with the private sector, which owns and operates many of these critical infrastructure facilities.

II. PDD-63--OVERVIEW

After releasing the PCCIP report, the Administration worked to incorporate these and other recommendations into Presidential Decision Directive 63, which was issued in May 1998. Most importantly, PDD-63 recognizes the need for a Public-Private Partnership to face these critical issues. The directive specifies sectors of the national infrastructure, primarily in the private sector, that provide critical services or functions. It designates lead agencies in the Federal Government to work as liaisons with their respective sectors to build partnerships. PDD-63 additionally recognizes that the traditional areas of national defense, foreign affairs, intelligence, and law enforcement are fundamental to infrastructure protection, are inherently the domain of the government, and stipulates that sector coordinators be designated for these areas from the associated government agencies.

PDD-63 established the position of National Coordinator for Security, Infrastructure Protection, and Counter Terrorism to orchestrate these efforts. The PDD lays out specific tasks that must be accomplished, time lines for doing so, and organizations for carrying out these missions. Key amongst them are the National Infrastructure Protection Center (NIPC), Directed by Mr. Vatis, and the National Plan Coordination Staff--now called the Critical Infrastructure Assurance Office (CIAO)--which I have the honor of directing.

PDD-63 focuses the nation's efforts on aspects of critical and immediate importance--and I emphasize that these must be the efforts of the whole nation, for success will come only from the efforts of the private sector, state and local governments, and the Federal Government working together in an integrated and cooperative manner. Our efforts

fall in three broad categories.

A. Defense and intelligence components

The first is the Federal Government agencies involved in defense and intelligence efforts. The armed forces and intelligence agencies have requirements and systems that are unique to their special role. This has long been recognized in law, in the way we structure these organizations, and in our national philosophy. Their efforts are, as would be expected from the sensitive and well established nature of their mission, much further along in achieving critical infrastructure protection than those of the other parts of the Federal Government. In many ways they have set the example for other agencies' efforts, and they currently share their experiences and advise on how the rest of the government might proceed. Their contribution has been very important in shaping the policy and programmatic reality the rest of the government is currently trying to establish. Mr. Richard Schaeffer, Director of the Information and Infrastructure Assurance Office for the Defense Department, has submitted a statement for the record on this and other matters, so, in cause of brevity, I will refer you to it and cover their efforts no further.

B. Government as model

The second category of effort can be called ``Government as a Model.'' We often say that more than 90 percent of our critical infrastructures are neither owned nor operated by the Federal Government. Partnerships with the private sector and State and Local Governments are therefore not just needed, but are the fundamental aspect of critical infrastructure protection. Yet, the President rightly challenged the Federal Government in PDD-63 to serve as a model for critical infrastructure protection--to put our own house in order first. As such, the Administration has focused what might appear to be a disproportionate amount of our effort early in the process on doing this by establishing a coordinated and integrated approach across the Federal Government.

Federal Computer Security Requirements and Government Infrastructure Dependencies

One component of this effort supports aggressive, government-wide implementation of federal computer security requirements. Thus, in support of PDD-63, the President forwarded to Congress a request for a fiscal year 2000 budget amendment that would enhance computer security and critical infrastructure protection in the Federal Government. This proposal would fund a permanent 15-member team at the Department of Commerce's National Institute of Standards and Technology (NIST) responsible for helping Agencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection Plans. The budget amendment would also establish an operational fund at NIST for computer security projects among Federal Agencies, including independent vulnerability assessments, computer intrusion drills, and emergency funds to cover security fixes for systems identified to have unacceptable security risks. Among others, the Director of the team

would consult with the Office of Management and Budget and the National Security Council on the team's plan to protect and enhance computer security for Federal Agencies.

Under PDD-63, the President directed the CIAO to coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. Many of the critical infrastructures that support our nation's defense and security are shared by multiple agencies. Even within government, then, critical infrastructure outages may cascade and unduly impair delivery of critical services. The CIAO is coordinating an interagency effort to develop a more sophisticated identification of critical nodes and systems and their impact on national security government-wide. These efforts will support the work of the ERT in identifying vulnerabilities of the government's computer infrastructures, planning secure computer systems, and implementing computer security plans.

This research, when complete, will provide important information to maximize national security research and development, budgeting, and for implementing Federal computer security requirements and critical infrastructure planning within each agency.

Federal Intrusion Detection Network (FIDNET)

PDD-63 marshals resources to improve interagency cooperation in detecting, and in responding to computer intrusions into civilian government critical infrastructure nodes. To support this effort, the Administration recently sent to Congress a fiscal year 2000 Budget Amendment to create a centralized intrusion detection and response capability in the General Services Administration (GSA). Through the use of additional staff and enhanced technology, Federal Agencies will improve upon their abilities to:

- detect computer attacks and unauthorized intrusions;
- share attack warnings and related information across agencies; and
- respond to attacks.

This amendment would provide GSA funds to pay for additional technology and personnel dedicated to intrusion detection and response. The additional personnel would improve Federal Agencies' ability to detect attacks, analyze data, and communicate attack information more swiftly, building on the existing Federal Computer Incident Response Capability (FedCIRC). The additional technology, in the form of state-of-the-art intrusion detection systems, would ensure a consistent capability in Agencies to protect critical systems.

The program--much like a centralized burglar alarm system--would operate within legal requirements and Government policy concerning privacy, civil liberties, and promoting confidence in users of Federal civilian computer systems. Attack and intrusion information would be gathered and analyzed by Agency experts. Only data on system anomalies would be forward to GSA for further analysis.

Neither the Federal Bureau of Investigation nor other law enforcement entities would receive information about the computer attacks and intrusions--except under long-standing legal rules and where an Agency determines there is sufficient indication of illegal

conduct. Also, private entities will not be wired to the FIDNet--no private sector entity is part of this civilian government program.

In short, FIDNet will be run by the GSA, not the FBI; will not monitor any private networks or email traffic; will confer no new authorities on any government agency; and will be fully consistent with privacy law and practice.

Education and Training

One of the nation's important shortcomings in our efforts to protect our critical infrastructures is a shortage of skilled information technology (IT) personnel. Within the subset of information systems security personnel, the shortage is acute. Within the Federal Government, the lack of skilled information systems security personnel amounts to a crisis. This shortfall of workers reflects a scarcity of university graduate and undergraduate information security programs. In attacking this problem, we will leverage the initial efforts made by the Defense Department, National Security Agency, and some Federal Agencies.

The Federal Cyber Services (FCS) training and education initiative introduces five programs to help solve the Federal IT security personnel problem.

- The Completion of an Office of Personnel Management IT occupational study. This study will help identify the number of IT security positions in the Federal Government, and the training and certification requirements for these positions.
- The development of Center(s) for Information Technology Excellence (CITE). These Centers will train and certify current Federal IT security personnel and maintain their skill levels throughout their careers. It will leverage the significant progress made by the Defense Department and other federal agencies on this issue.
- The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT security workers and managers. This program will fund up to 300 students per year in their pursuit of undergraduate or graduate degrees in the IT security field. In return, the students will serve in the Federal IT workforce for a fixed period following graduation. The program will also have a meaningful summer work and internship element. An important part of the SFS program is the need to identify universities for participation in the program and assist in the development of IT security faculty and laboratories at these universities.
- The development of a high school recruitment and training initiative. This program would identify promising high school students for participation in summer work and internship programs that would lead to certification to Federal IT workforce standards and possible future employment. This effort will also examine possible programs to promote computer security awareness in secondary and high school classrooms.
- The development and implementation of a Federal INFOSEC awareness curriculum. This awareness effort is aimed at ensuring the entire Federal workforce is developing computer

security literacy. It will leverage several outstanding existing federal agency awareness programs.

Research and Development

A key component to our ability to protect our critical infrastructures now and in the future is a robust research and development plan. The interagency Critical Infrastructure Coordination Group (CICG) has created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works with Agencies and the private sector to:

- gain agreement on requirements and priorities for information security research and development;
- coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;
- communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and
- identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, led to the Administration budget request for fiscal year 2000 of $500 million for critical infrastructure protection research. Among the priorities identified by the process are:

- technology to support large-scale networks of intrusion detection monitors;
- artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;
- methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster;
- technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and
- technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

C. Public-private partnership

Thirdly, and as discussed above, one of the most important components of PDD-63 implementation is the development of collaborative partnerships among and between the private sector, state and local governments, and the Federal Government. The importance of this effort cannot be overstated and is made clear by considering just a few scenarios. If the natural gas delivery system you rely on for heat and cooking fails in January due to an attack on the computer systems that

direct its operations, you will take small comfort in fact that the Federal Government has a critical infrastructure protection plan in place. In fact, all our efforts to put the Federal Government's house in order and to serve as a model for industry will be of little service if our government information systems are impossible to break into, but the electrical power that they operate on is shut down by malicious actions of a foreign government. The list of examples goes on and on, and none of these systems is owned or operated by the Federal Government.

These vignettes put the situation in perspective--we are faced with a fascinating and challenging problem. This is the first time I am aware of in our national history that by creating policy and expending resources, the Federal Government cannot alone solve a national security problem. So what are we doing about it? If by ``we'' you understand ``the government'' then the answer must necessarily be unsatisfactory--because the government alone cannot protect the nation's infrastructures. But if by ``we'' you understand ``the nation''--the Federal Government in a coordinated and integrated effort with state and local government, industry, academia and other concerned groups--then I am happy to report that we have made a good beginning, and are developing a strong future.

Just last Friday, Treasury Secretary Summers announced the formation of the Financial Sector Information Sharing and Analysis Center--``ISAC'' for short. ISAC's are private sector owned and operated entities that serve as focal points for their associated sector of the economy. Because they are defined individually by their member organizations, they will not all be identical. They are, however, all to be the coordinating and analyzing body for cyber attacks on their specific sector. I want to emphasize that these ISAC's are neither set up, nor supervised by the Federal Government, although the Federal Government will assist these critical sectors in setting up their ISAC, through the Sector Liaisons, if asked. The government will share what information we can on cyber attacks with the ISAC's to help them protect their sector, and we will encourage them to share appropriately sanitized information with us to help us protect government agencies and functions. But this sharing from ISAC's to government will be on an entirely voluntary basis, both in amount of information and the level of detail. No requirement exists or will exist that mandates information sharing.

While these ISAC's, would work within the sectors of the economy that own and operate critical infrastructure, as stipulated in PDD-63, this is not intended to be limiting. Other sectors or groupings within industry could establish ISAC's, and we would assist them in this. Furthermore, practically every aspect of our nation relies on critical infrastructures. This makes CIP a fundamentally important issue for not just those companies that own and operate critical infrastructure, but also for those that rely on it to do business. They can and must have a voice in this public/private partnership.

Recently, the President issued an Executive Order establishing a National Infrastructure Assurance Council (NIAC). This Presidential advisory body will be comprised of leaders from the Private Sector, State and Local governments, and the Federal Government. It will examine key aspects of critical infrastructure assurance, and report to the President.

The final indispensable members of this partnership are state and local governments. They have the fundamentally important roles of providing and regulating many if not most essential services. They are the front line forces in the event of disasters or attacks on infrastructures. Some have moved quite far in their critical infrastructure protection efforts--New Mexico, for example, under the direction of Dr. Dan O'Neil, has a very strong and growing critical infrastructure protection partnership with key private sector entities. Furthermore, we have long had strong relationships with state and local governments on specific issues related to critical infrastructure protection, such as state and local emergency management organizations with FEMA, and state and local law enforcement agencies through the FBI and other national law enforcement agencies. This area is one in which much work remains to be done, and I look forward to working with each Congressional Delegation as we define the issues and solutions.

III. CONCLUSION

In conclusion, much has been done since PDD-63 was issued in 1998. My staff and I are committed to building on this promising beginning, coordinating the government's efforts into an integrated holistic program for critical infrastructure protection under the direction of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. We have much work left to do, and I look forward to with the members of this committee, indeed with the Congress as a whole, as we wrestle with this developing field and implement solutions. I look forward to your questions.

Senator Kyl. Mr. Vatis.

STATEMENT OF MICHAEL A. VATIS

Mr. Vatis. Mr. Chairman, Senator Feinstein and Senator Bennett, thank you very much for inviting me here this morning to speak with you about critical infrastructure protection. You three have really been leaders in the Congress in recognizing the importance of these issues and the urgency of dealing with the new cyber threat that we face now in the information age, and so it is a privilege to share our perspective with you all, coming from the NIPC.

I think your statements, your three statements, have really laid out the issue quite nicely in terms of the threats that we face and why our vulnerabilities are so great in this area, so I think I would like to focus my brief oral remarks on our perspective on the threats and how we are approaching them and attempting to deal with them.

Much of the news media accounts on this issue focus on hacks into government websites and some private sector websites, and while those are criminal acts and they are not unimportant, they are not really where the main threat lies. The main threat lies in the potential for foreign nation states, foreign actors, and also domestic actors to hack into the critical computer networks that control our Nation's vital infrastructures, the services that are essential to the basic

functioning of our economy and are essential to our national security, such as the telecommunications network, the electrical power grid, government operations, other energy systems, banking and finance, et cetera. Those are what we refer to as our critical infrastructures and those are the things that we are focused on protecting from attack.

Mr. Chairman, you mentioned recent media accounts of a significant series of intrusions into Department of Defense and other government agency networks. This is a matter that we have been looking into for over a year now and it points up for those who needed yet another wake-up call the serious vulnerabilities that we are trying to deal with and the serious threats that we are facing, not 5 or 10 years in the future, but today. These are threats to our national security that we must confront now because it is already happening.

As you mentioned, Mr. Chairman, the greatest potential threat comes from foreign state actors who might choose to engage in information warfare against the United States because they realize that they cannot take us on in conventional military terms and would seek to go after what they perceive as our Achilles heel, as you put it, which is our reliance on information technology, more than any other country, to control our critical operations.

Information warfare is not the only threat. There is also a threat from foreign nation states engaged in cyber espionage, using remote access that is afforded by the interconnectivity of the Internet and our telecommunications systems, to access sensitive government information or sensitive private sector information, essentially engaged in industrial or economic espionage, to steal secrets to advantage their own indigenous industries at the expense of our own American private sector. These are threats, again, that are not just future threats, but they are threats that we must deal with right now.

On the non-state side, there are a variety of bad actors who can engage in similar types of intrusions for different purposes, but essentially using very similar, if not the same, techniques. We have seen terrorist groups beginning to acquire both the equipment and the expertise to use information technology as a weapon. For some time now, we have seen terrorist groups using the Internet and other forms of information technology to raise funds, to spread propaganda, and to communicate securely using encryption.

More recently, we have begun to see terrorists now focusing on using those same set of technologies as a weapon. We have seen the Internet Black Tigers associated with the Tamil Tigers, engage in a denial of service attack on e-mail servers of Sri Lankan government embassies. We also have concerns that Aum Shinrikyo, the Japanese terrorist group that launched the deadly sarin gas attack in Tokyo, beginning to think about using its expertise in computers and in networks as a possible weapon to direct against Japanese or U.S. interests. And there are reports that traditional terrorist groups such as the IRA have thought about using these same sorts of tools as weapons against their intended targets.

All of these factors really portend the possibility and likelihood of a serious cyber terrorist attack directed against U.S. interests, but right now, we are already seeing criminal groups using these tools, not necessarily to disrupt systems, but to steal money, which is what criminal groups are basically all about.

We have had the example that is now 5 years old of a Russian organized crime group headquartered in St. Petersburg using the same types of techniques to break into the Citibank cash management system and start transferring over $10 million to their own accounts. Fortunately, Citibank contacted the FBI early on and Citibank was able to stem its losses at approximately $400,000. All of the members of the group were apprehended and eventually prosecuted.

But we still face that similar problem from criminal groups. The Phonemasters case that you mentioned, Mr. Chairman, is just another example of a group that does not fit our common definition of an organized crime group, but it was a group, it was organized, and it engaged in serious criminal activity. So I think we need to open our minds to some new paradigms out there of organized crime, people who are perhaps younger than our typical vision of organized crime groups but are taking advantage of these new technologies to engage in serious fraud schemes, serious theft schemes, and other types of criminal conspiracies.

But we have also seen individuals posing a serious threat. In the last year alone, we have seen at least three very serious viruses or worms, the Melissa virus, the Explore.zip worm, the Chernobyl virus, wreak serious havoc on the private sector, some estimates going into the hundreds of millions of dollars of damage caused to private companies from the disruption caused by these viruses.

We have also seen what we call recreational hackers cause serious harm, individuals who may be engaged in hacking just for the thrill of it, as Senator Feinstein said, or for bragging rights in the hacker community because they are a competitive bunch who like to show that they are better than the other guy. But they can have very serious consequences in their hacks. It is not just benign fun, as it is sometimes portrayed to be.

We had an example a couple of years ago of a teenager in Massachusetts who hacked into the then-NYNEX, now Bell Atlantic telephone system, and shut down telecommunications in the Worcester, MA, area for several thousand users. What he did not intend was that he also disrupted communications to the local airport and prevented incoming airplanes from communicating with the tower and from turning on the runway lights. That could have obviously had very serious impacts on the safety of people using that airport. He also had the effect of shutting down communications of local police and rescue services. So even things that might seem relatively benign can have very serious impacts on our public safety.

The final category of individuals is probably the most common, and that is the disgruntled insider, an employee or

former employee at a company who abuses his knowledge and access to a system to cause disruption, by causing the system to crash because he is angry at his employer, by stealing sensitive information and giving it to a competitor, or altering information. We have countless examples of these types of instances and that is probably the category that the private sector is most concerned about. Fifty-five percent of respondents in a recent poll by the Computer Security Institute and the FBI said that they had insider problems, insiders accessing their systems and doing bad things.

So there is an incredibly broad array of threats in the cyber area that we have to deal with, and one of the difficulties in this area that distinguishes it qualitatively from the physical world is that when you first notice that you have an intrusion, you do not know what you are dealing with. You do not know if it is a disgruntled insider, if it is an organized crime group, if it is a terrorist, a foreign intelligence agency, or a nation state planting the seeds for future destructive attacks.

And as a result, because you do not know how to deal with it, in the government, it is not clear who should have responsibility, as Senator Bennett said, because it is not clear what you are dealing with. If we knew it were a nation state engaged in preparing the battlefield for an information warfare attack, then clearly a military response might be called for. But if we do not know that going in, it is hard to assign responsibility.

In the Solar Sunrise case that I think all three of you alluded to from February 1998, it looked at first blush like it might be an instance of information warfare attack by the Iraqi government because we were deploying troops to the Gulf at the time and some of the attacks seemed to be coming through Internet service providers in the Gulf region. Upon investigation, however, we determined that the intrusions were carried out by several teenagers, two in California and several more in Israel. So what looked like a possible information warfare attack ended up being recreational hackers who were hacking for the thrill of it.

As a result of that difficulty of knowing what you are dealing with, who is doing it, how are they getting in, why are they doing it, what systems are they affecting, and where are they coming from, the response that the Federal Government took in PDD 63 was to create an interagency center at the NIPC, located at the FBI, but with representatives from all of the agencies who have a role to play, depending on what we determine we are confronting. So we have representatives at senior levels, at analytical levels, and on the investigative side, as well, from the Department of Defense, from the intelligence community, from other Federal law enforcement agencies, until recently, from State and local law enforcement, and eventually, we hope to have representatives from the private sector brought in, as well.

So as we investigate a case and can make determinations about who is doing what to us, we can have quick hand-off to

the appropriate agencies that have responsibility. But the reason for putting the NIPC under the auspices of the FBI is because to make those determinations, we need to gather information from the victim sites, from some of the intermediate sites that might have been attacked on the way to the ultimate victim, and the only way legally we can gather that information is pursuant to law enforcement investigative authorities, or in some more narrow circumstances, counterintelligence authorities, if we know going in that this is a nation state-sponsored attack.

But once we gather that information using those legal authorities, the ultimate response and the ultimate responsibility for dealing with it will depend on the facts, and at that point, other agencies would have a more direct role to play, be it a military response, a diplomatic response, an intelligence response, or a law enforcement response.

Let me just say, finally, since I have used up all my time and more, that we are looking at Y2K as yet another example of how we need to coordinate, particularly on the information sharing side. Our responsibility at the NIPC is not to deal with service outages caused by the millennium bug and the inability of computers to recognize the date change. Our focus is, just as it is every day, is on dealing with malicious criminal attacks, intrusions or viruses that people use to attack systems. We do not have any concrete information indicating that any foreign group or domestic group is planning on engaging in these sorts of attacks specifically around Y2K, but we are preparing for that eventuality because of the distinct possibility that people might see as an opportunity to engage in those sorts of attacks.

So in our field offices across the country and here at FBI headquarters, the NIPC is preparing a contingency plan to deal with those sorts of attacks, and we have been communicating very closely with the rest of the Federal community, with State and local governments, and with the new Information Coordination Center at the White House, which is dealing with the Y2K problem overall and focusing on sharing information about the state of critical systems during the rollover period.

That concludes my somewhat lengthier remarks that I had intended, but I hope that gave you some insight into how we approach the problem.

Senator Kyl. Thank you very much, Mr. Vatis.

[The prepared statement of Mr. Vatis follows:]

PREPARED STATEMENT OF MICHAEL A. VATIS

INTRODUCTION

Mr. Chairman, Senator Feinstein, and Members of the Committee: Thank you for inviting me here today to discuss critical infrastructure protection issues. Mr. Chairman, you and this committee have been leaders in recognizing the importance of these issues and the urgency of addressing the new threats to our national security in the Information Age, and I welcome this opportunity to share our

perspectives with you today. As you know, the Federal Government is developing its capabilities for dealing with threats to our nation's infrastructures. Presidential Decision Directive-63 set in motion an unprecedented effort to protect our nation's critical infrastructures, which the PDD defined as ``those physical and cyber-based systems essential to the minimum operations of the economy and government.'' Critical infrastructures include telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both public and private. The PDD formally designated the National Infrastructure Protection Center (NIPC) to have a central operational role in the government's effort. The Center works closely with the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism; the Department of Defense (DOD); the U.S. Intelligence Community (USIC); other federal agencies; and the private sector to protect our critical infrastructures. My statement will cover the spectrum of threats we are facing and the status of the NIPC and its activities.

SPECTRUM OF THREATS

The news media is filled with examples of intrusions into government and private sector computer networks. Politically motivated hackers have been attacking numerous U.S. Government websites, including the Senate's. Deputy Secretary of Defense John Hamre reported in February that DOD is ``detecting 80 to 100 [potential hacking] events daily.'' We have had several damaging computer viruses this year, including the Melissa Macro Virus, the Explore.Zip Worm, and the CIH (Chernobyl) Virus. Computer Economics, Inc., a California firm, estimates that damage in the first two quarters of 1999 from viruses has topped $7 billion. The FBI's case load for computer hacking and network intrusion cases has doubled each of the last two years. Currently we have over 800 pending investigations. In its 1999 survey, the Computer Security Institute estimated the total financial losses by the 163 businesses it surveyed from computer security breaches at $123.7 million. This includes everything from theft of proprietary data to denial of service on networks. E-commerce has become so important that firms, including Sedgwick Group PLC (in cooperation with IBM), Lloyds of London, and Network Risk Management Services, are now offering ``hacker insurance.''

Sensitive intrusions

In the past few years we have seen a series of intrusions into numerous Department of Defense computer networks as well as networks of other federal agencies, universities, and private sector entities. Intruders have successfully accessed U.S. Government networks and took large amounts of unclassified but sensitive information. In investigating, these cases, the NIPC has been coordinating with FBI Field Offices, the Department of Defense, and other government agencies, as circumstances require. But it is important that the Congress and the American public understand the very real threat that we are facing in the cyber realm, not just in the future, but now.

Information warfare

Perhaps the greatest potential threat to our national security is the prospect of ``information warfare'' by foreign militaries against our critical infrastructures. We know that several foreign nations are

already developing information warfare doctrine, programs, and capabilities for use against each other and the United States or other nations. Foreign nations are developing information warfare programs because they see that they cannot defeat the United States in a head-to-head military encounter and they believe that information operations are a way to strike at what they perceive as America's Achilles Heel--our reliance on information technology to control critical government and private sector systems. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. In addition, during the recent conflict in Yugoslavia, hackers sympathetic to Serbia electronically ``ping'' attacked NATO web servers. And Russian as well as other individuals supporting the Serbs attacked websites in NATO countries, including the United States, using virus-infected e-mail and hacking attempts. Over 100 entities in the United States received these e-mails. Several British organizations lost files and databases. These attacks did not cause any disruption of the military effort, and the attacked entities quickly recovered. But such attacks are portents of much more serious attacks that we can expect foreign adversaries to attempt in future conflicts.

Foreign intelligence services

Foreign intelligence services have adapted to using cyber tools as part of their information gathering and espionage tradecraft. In a case dubbed ``the Cuckoo's Egg,'' between 1986 and 1989 a ring of West German hackers penetrated numerous military, scientific, and industry computers in the United States, Western Europe, and Japan, stealing passwords, programs, and other information which they sold to the Soviet KGB. Significantly, this was over a decade ago--ancient history in Internet years. While I cannot go into specifics about the situation today in an open hearing, it is clear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information.

Terrorists

Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. For example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. Moreover, some groups have already used cyber attacks to inflict damage on their enemies' information systems. For example, a group calling itself the Internet Black Tigers conducted a successful ``denial of service'' attack on servers of Sri Lankan government embassies. Italian sympathizers of the Mexican Zapatista, rebels attacked web pages of Mexican financial institutions. And a Canadian government report indicates that the Irish Republican Army has considered the use of information operations against British interests. We are also concerned that Aum Shinrikyo, which launched the deadly Sarin gas attack in the Tokyo subway system, could use its growing expertise in computer manufacturing and Internet technology to develop ``cyber terrorism''

weapons for use against Japanese and U.S. interests. Thus while we have yet to see a significant instance of ``cyber terrorism'' with widespread disruption of critical infrastructures, all of these facts portend the use of cyber attacks by terrorists to cause pain to targeted governments or civilian populations by disrupting critical systems.

Criminal groups

We are also beginning to see the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. For example, in 1994 the U.S. Secret Service uncovered a $50 million phone card scam that abused the accounts of AT&T, MCI, and Sprint customers. In addition, in 1994-95 an organized crime group headquartered in St. Petersburg, Russia, transferred $10.4 million from Citibank into accounts all over the world. After surveillance and investigation by the FBI's New York field office, all but $400,000 of the funds were recovered. In another case, Carlos Felipe Salgado, Jr. gained unauthorized access to several Internet Service Providers in California and stole 100,000 credit card numbers with a combined limit of over $1 billion. The FBI arrested him in the San Francisco International Airport when he tried to sell the credit card numbers to a cooperating witness for $260,000. With the expansion of electronic commerce, we expect to see an increase in hacking by organized crime as the new frontier for large-scale theft.

Just two weeks ago, two members of a group dubbed the ``Phonemasters'' were sentenced after their conviction for theft and possession of unauthorized access devices (18 USC Sec. 1029) and unauthorized access to a federal interest computer (18 USC Sec. 1030). The ``Phonemasters'' are an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the FBI's National Crime Information Center (NCIC). Under judicially approved electronic surveillance orders, the FBI's Dallas Field Office made use of new data intercept technology to monitor the calling activity and modem pulses of one of the suspects, Calvin Cantrell. Mr. Cantrell downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual, who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Mr. Cantrell was sentenced to two years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

The ``Phonemasters'' activities should serve as a wake up call for corporate security. Their methods included ``dumpster diving'' to gather old phone books and technical manuals for systems. They then used this information to trick employees into giving up their logon and password information. The group then used this information to break into victim systems. It is important to remember that often ``cyber crimes'' are facilitated by old fashioned guile, such as calling employees and tricking them into giving up passwords. Good ``cyber security'' practices must therefore address personnel security and ``social engineering'' in addition to instituting electronic security measures.

Virus writers

Virus writers are posing an increasingly serious threat to networks and systems worldwide. As noted above, we have had several damaging computer viruses this year, including the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus. The NIPC frequently sends out warnings regarding particularly dangerous viruses.

Earlier this year, we reacted quickly to the spread of the Melissa Macro Virus. While there are dozens of viruses released every day, the speedy propagation of Melissa and its effects on networks caused us great concern. Within hours of learning about the virus on Friday, March 26, 1999, we had coordinated with key cyber response components of DOD and the Computer Emergency Response Team (CERT) at Carnegie-Mellon University. Our Watch operation went into 24-hour posture and sent out warning messages to federal agencies, state and local law enforcement, FBI Field Offices, and the private sector. Because the virus affected systems throughout the public, we also took the unusual step of issuing a public warning through the FBI's Public Affairs Office and on our website. These steps helped mitigate the damage by alerting computer users of the virus and of protective steps they could take.

On the investigative side, the NIPC acted as a central point of contact for the Field Offices who worked leads on the case. A tip received by the New Jersey State Police from America Online, and their follow-up investigation with the FBI's Newark Field Office, led to the April 1, 1999 arrest of David L. Smith. Search warrants were executed in New Jersey by the New Jersey State Police and FBI Special Agents from the Newark Field Office.

Just in the last few weeks we have seen reports on the Suppl Word Macro virus, the toadie.exe virus, and the W97M/Thurs.A (or Thursday) virus., This last virus has already infected over 5,000 machines, according to news reports, and deletes files on victim's hard drives. The payload of the virus is triggered on 12-13 and disables the macro virus protection in Word 97. We are also concerned with the propagation of a Trojan Horse called Back Orifice 2000, which allows malicious actors to monitor or tamper with computers undetected by the users.

Virus writers are not often broken out as a threat category, and yet they often do more damage to networks than hackers do. The prevalence of computer viruses reminds us that we all have to be very careful about the attachments we open and we all must be sure to keep our anti-virus software up-to-date.

Hactivism

Recently we have seen a rise in what has been dubbed ``hacktivism''--politically motivated attacks on publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into web sites to send a political message. While these attacks generally have not altered operating systems or networks, they still damage services and deny the public access to websites containing valuable information and infringe on others' right to communicate. One such group is called the ``Electronic Disturbance Theater,'' which promotes civil disobedience on-line in support of its political agenda regarding the Zapatista movement in Mexico and other issues. This past spring they called for worldwide electronic civil

disobedience and have taken what they term ``protest actions'' against White House and Department of Defense servers. Supporters of Kevin Mitnick, recently convicted of numerous computer security offenses, hacked into the Senate webpage and defaced it in May and June of this past year. The Internet has enabled new forms of political gathering and information sharing for those who want to advance social causes; that is good for our democracy. But illegal activities that disrupt e-mail servers, deface web-sites, and prevent the public from accessing information on U.S. government and private sector web sites should be regarded as criminal acts that deny others their First Amendment rights to communicate rather than as an acceptable form of protest.

``Recreational'' hackers

Virtually every day we see a report about ``recreational hackers,'' or ``crackers,'' who crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, the recreational hacker can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use.

These types of hacks are very numerous and may appear on their face to be benign. But they can have serious consequences. A well-known example of this involved a juvenile who hacked into the NYNEX (now Bell Atlantic) telephone system that serviced the Worcester, Massachusetts area using his personal computer and modem. The hacker shut down telephone service to 600 customers in the local community. The resulting disruption affected all local police and fire 911 services as well as the ability of incoming aircraft to activate the runway lights at the Worcester airport. Telephone service was out at the airport tower for six hours. The U.S. Secret Service investigation of this case also brought to light a vulnerability in 22,000 telephone switches nationwide that could be taken down with four keystrokes. Because he was a juvenile, however, the hacker was sentenced to only two years probation and 250 hours of community service, and was forced to forfeit the computer equipment used to hack into the phone system and reimburse the phone company for $5,000. This case demonstrated that an attack against our critical communications hubs can have cascading effects on several infrastructures. In this case, transportation, emergency, services, and telecommunications were disrupted. It also showed that widespread disruption could be caused by a single person from his or her home computer.

Insider threat

The disgruntled insider is a principal source of computer crimes. Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of victim systems often allows them to gain unrestricted access to cause damage to the system or to steal system data. The 1999 Computer Security Institute/FBI report notes that 55 percent of respondents reported malicious activity by insiders.

There are many cases in the public domain involving disgruntled insiders. For example, Shakuntla Devi Singla used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency

employees over 1,800 hours to recover and reenter the lost data. Ms. Singla was convicted and sentenced to five months in prison, five months home detention, and ordered to pay $35,000 in restitution.

In another case, a former Forbes employee named George Parente hacked got into Forbes systems using another employee's password and login identification and crashed over half of Forbes' computer network servers and erased all of the data on each of the crashed services. The data could not be restored. The losses to Forbes were reportedly over $100,000.

Identifying the intruder

One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking your system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. The now well known ``Solar Sunrise'' case illustrates this point. Solar Sunrise was a multi-agency investigation (which occurred while the NIPC was being established) of intrusions into more than 500 military, civilian government, and private sector computer systems in the United States, during February and March 1998. The intrusions occurred during the build-up of United States military personnel in the Persian Gulf in response to tension with Iraq over United Nations weapons inspections. The intruders penetrated at least 200 unclassified U.S. military computer systems, including seven Air Force bases and four Navy installations, Department of Energy National Laboratories, NASA sites, and university sites. Agencies involved in the investigation included the FBI, DOD, NASA, Defense Information Systems Agency, AFOSI, and the Department of Justice.

The timing of the intrusions and links to some Internet Service Providers in the Gulf region caused many to believe that Iraq was behind the intrusions. The investigation, however, revealed that two juveniles in Cloverdale, California and several individuals in Israel were the culprits. Solar Sunrise thus demonstrated to the interagency community how difficult it is to identify an intruder until facts are gathered in an investigation, and why assumptions cannot be made until sufficient facts are available. It also vividly demonstrated the vulnerabilities that exist in our networks; if these individuals were able to assume ``root access'' to DOD systems, it is not difficult to imagine what hostile adversaries with greater skills and resources would be able to do. Finally, Solar Sunrise demonstrated the need for interagency coordination by the NIPC.

Special threat: Y2K malicious activity

The main concern with the Y2K rollover is, of course, the possibility of widespread service outages caused by the millennium date problem in older computer systems. The President's Y2K Council has done an excellent job in helping the nation prepare for the rollover event. Given our overall mission under PDD 63, the NIPC's role with regard to Y2K will be to maintain real-time awareness of intentional cyber threats or incidents that might take place around the transition to 2000, disseminate warnings to the appropriate government and private

sector parties, and coordinate the government's response to such incidents. We are not responsible for dealing with system outages caused by the millennium bug. Because of the possibility that there might be an increase in malicious activity around January 1, 2000, we have formulated contingency plans both for NIPC Headquarters and the

FBI Field Offices.

We are presently augmenting our existing relationships and information-sharing mechanisms with relevant entities in the federal government, such as the Information Coordination Center (ICC), state and local governments, private industry, and the CERT/FIRST community. Information will come to us from a variety of places, including FBI field offices and Legal Attaches overseas, as well as the ICC. FBI field offices are also tasked to establish Y2K plans for their regions of responsibility. In essence, all of the activities that we will undertake during the rollover period are ones we perform everyday. The difference is that we will be prepared to conduct them at an increased tempo to deal with any incidents occurring during the Y2K rollover.

There is one potential problem associated with Y2K that causes us special concern--the possibility that malicious actors, foreign or domestic, could use the Y2K remediation process to install malicious code in the ``remediated'' software. Thousands of companies across the United States and around the world are busy having their source code reviewed to ensure that they are ``Y2K compliant.'' Those who are doing the Y2K remediation are almost always contractors who are given the status of a trusted insider with broad authority to review and make changes to the source code that runs information systems. These contractors could, undetected, do any of the following to compromise systems:

- Install Trap Doors: By installing trap doors, intruders can later gain access to a system through an opening that they have created and then exploit or attack the system;
- Obtain ``Root Access'': Given their level of access, remediation companies can gain the same extensive privileges as the system administrator, allowing them to steal or alter information or engage in a ``denial of service'' attack on the system.
- Implant Malicious Code: By implanting malicious code, someone could place a logic bomb or a time-delayed virus in a system that will later disrupt it. A malicious actor could also implant a program to compromise passwords or other aspects of system security.
- Map Systems: By mapping systems as a trusted insider, a contractor can gain valuable information to sell to economic competitors or even foreign intelligence agencies.

Systems can be compromised for any number of purposes, including foreign intelligence activities, information warfare, industrial espionage, terrorism, or organized crime. And since any vulnerabilities that are implanted will persist as long as the software is in place, this is a problem that will last well beyond January 1, 2000. Companies and government agencies therefore need to determine how they will deal

with this potential ``Post-Y2K problem'' on their critical systems.

We have little concrete evidence so far of vendors' planting malicious code during remediation. But the threat is such that companies should take every precaution possible. Of course, checking the remediation work to make sure that no malicious code was implanted in a system is no easy matter. If reviewing the millions of lines of code at issue were simple, there would be little need for Y2K contractors in the first place. Nevertheless, given the vulnerabilities that could be implanted in critical systems, it is imperative that the client companies do as much as possible to check the background of the companies doing their remediation work, oversee the remediation process closely, and review new code as closely as possible and remove any extraneous code. Further, companies should test for trap doors and other known vulnerabilities to cracking. Companies can also use ``red teams'' to try to crack the software and further determine if trap doors exist.

STATUS OF THE NIPC

The NIPC is an interagency Center located at the FBI. Created in 1998, the NIPC serves as the focal point for the government's efforts to warn of and respond to cyber intrusions. In PDD-63, the President directed that the NIPC ``serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.'' The PDD further states that the mission of the NIPC ``will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.''

Thus, the PDD places the NIPC at the core of the government's warning, investigation, and response system for threats to, or attacks on, the nation's critical infrastructures. The NIPC is the focal point for gathering information on threats to the infrastructures as well as ``facilitating and coordinating the Federal Government's response to an incident.'' The PDD further specifies that the NIPC should include ``elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach, and development and application of technical tools.''

The NIPC has a vital role in collecting and disseminating information from all relevant sources. The PDD directs the NIPC to ``sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state, and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity.'' The NIPC is also charged with issuing ``attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators.''

In order to perform its role, the NIPC is continuing to establish a network of relationships with a wide range of entities in both the government and the private sector. The PDD provides for this in several ways. First, it states that the Center will ``include representatives from the FBI, U.S. Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, Intelligence

Community and Lead Agencies.'' \1\ Second, pursuant to the PDD, the NIPC has electronic links to the rest of the government in order to facilitate the sharing of information and the timely issuance of warnings. Third, the PDD directs all executive departments and agencies to ``share with the NIPC information about threats and warning of attacks and actual attacks on critical government and private sector infrastructures, to the extent permitted by law.'' By bringing other agencies directly into the Center and building direct communication linkages, the Center provides a means of coordinating the government's cyber expertise and ensuring full sharing of information, consistent with applicable laws and regulations.

\1\ The Lead Agencies are: Commerce for information and communications; Treasury for banking and finance; EPA for water supply; Transportation for aviation, highways, mass transit, pipelines, rail, and waterborne commerce; Justice/FBI for emergency law enforcement services; Federal Emergency Management Agency for emergency fire service and continuity of government; Health and Human Services for public health services. The Lead Agencies for special functions are: State for foreign affairs, CIA for intelligence, Defense for national defense, and Justice/FBI for law enforcement and internal security. The NIPC is performing the lead agency and special functions roles specified for ``Justice/FBI'' in the PDD.

To accomplish its goals under the PDD, the NIPC is organized into three sections:

The Computer Investigations and Operations Section (CIOS) is the operational and response arm of the Center. It program manages computer intrusion investigations conducted by FBI Field Offices throughout the country; provides subject matter experts, equipment, and technical support to cyber investigators in federal, state, and local government agencies involved in critical infrastructure protection; and provides a cyber emergency response capability to help resolve a cyber incident.

The Analysis and Warning Section (AWS) serves as the ``indications and warning'' arm of the NIPC. The AWS reviews numerous government and private sector databases, media, and other sources daily to disseminate information that is relevant to any aspect of NIPC's mission, including the gathering of indications of a possible attack. It provides analytical support during computer intrusion investigations, performs analyses of infrastructure risks and threat trends, and produces current analytic products for the national security and law enforcement communities, the owners-operators of the critical infrastructures, and the computer network managers who protect their systems. It also distributes tactical warnings, alerts, and advisories to all the relevant partners, informing them of exploited vulnerabilities and threats.

The Training, Outreach and Strategy Section (TOSS) coordinates the training and continuing education of cyber investigators within the FBI Field Offices and other federal, state and local law enforcement agencies. It also coordinates

our liaison with private sector companies, state and local governments, other government agencies, and the FBI's Field Offices. In addition, this section manages our collection and cataloguing of information concerning ``key assets''--i.e., critical individual components within each infrastructure sector, such as specific power grids, telecommunications switch nodes, or financial systems--across the country.

To facilitate our ability to investigate and respond to attacks, the FBI has created the National Infrastructure Protection and Computer Intrusion (NIPCI) Program in the 56 FBI Field Offices across the country. Under this program, managed by the NIPC at FBIHQ, ``NIPCI'' squads consisting of at least seven agents have been created in 10 Field Offices: Washington D.C., New York, San Francisco, Chicago, Dallas, Los Angeles, Atlanta, Charlotte, Boston, and Seattle. For fiscal year 2000, we intend to reallocate our existing field agent compliment to create six additional squads in Baltimore, Houston, Miami, Newark, New Orleans, and San Diego. Because of resource constraints, the other field offices have only 1-5 agents dedicated to working NIPCIP matters.

The NIPC's mission clearly requires the involvement and expertise of many agencies other than the FBI. This is why the NIPC, though housed at the FBI, is an interagency center that brings together personnel from all the relevant agencies. In addition to our 79 FBI employees, the NIPC currently has 28 representatives from: DOD (including the military services and component agencies), the CIA, DOE, NASA, the State Department as well as federal law enforcement, including the U.S. Secret Service, the U.S. Postal Service and, until recently, the Oregon State Police. The NIPC is in the process of seeking additional representatives from State and local law enforcement.

But clearly we cannot rely on government personnel alone. Much of the technical expertise needed for our mission resides in the private sector. Accordingly, we rely on contractors to provide technical and other assistance. We are also in the process of arranging for private sector representatives to serve in the Center full time. In particular, the Attorney General and the Information Technology Association of America (ITAA) announced in April that the ITAA would detail personnel to the NIPC as part of a ``Cybercitizens Partnership'' between the government and the information technology (IT) industry. Information technology industry representatives serving in the NIPC would enhance our technical expertise and our understanding of the information and communications infrastructure.

NIPC activities

The NIPC's operations can be divided into three categories: protection, detection, and response.

Protection

Our role in protecting infrastructures against cyber intrusions is not to advise the private sector on what hardware or software to use or to act as their systems administrator. Rather, our role is to provide

information about threats, ongoing incidents, and exploited vulnerabilities so that government and private sector system administrators can take the appropriate protective measures. The NIPC is developing a variety of products to inform the private sector and other government agencies of threats, including: warnings, alerts, and advisories; the Infrastructure Protection Digest; Critical Infrastructure Developments; CyberNotes; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, the Infrastructure Protection Digest is a quarterly publication providing analyses and information on critical infrastructure issues. The Digest provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in both classified and unclassified formats and reaches national security and civilian government agency officials as well as infrastructure owners. Critical Infrastructure Developments is distributed bi-weekly to private sector entities. It contains analyses of recent trends, incidents, or events concerning critical infrastructure protection. CyberNotes is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and critical infrastructure-related best practices. It is published twice a month on our website and disseminated in hard copy to government and private sector audiences.

The NIPC, in conjunction with the private sector, has also developed an initiative called ``InfraGard'' to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions and exploited vulnerabilities, with the goal of increasing protection of critical infrastructures. The initiative encourages the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The initiative includes an intrusion alert network using encrypted e-mail, a secure website and local chapter activities. A critical component of InfraGard is the ability of industry to provide information on intrusions to the NIPC and the local FBI Field Office using secure communications in both a detailed and a ``sanitized'' format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation, while the NIPC can analyze that information in conjunction with law enforcement, intelligence, open source, or other industry information to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. InfraGard also provides us with a regular, secure method of providing additional security related to information to the private sector based on information we obtained from law enforcement investigations and other sources. InfraGard has recently been expanded to a total of 21 FBI Field Offices. The program will be expanded to the rest of the country later this year.

Under PDD-63, the NIPC also serves as the U.S. governments ``Lead Agency'' for the Emergency Law Enforcement Services Sector. As Sector

Liaison for law enforcement, the NIPC and a ``Sector Coordinator'' committee representing state and local law enforcement are formulating a plan to reduce the vulnerabilities of state and local law enforcement to cyber attack and are developing methods and procedures to share information within the sector. The NIPC and the FBI Field Offices are also working with the State and local law enforcement agencies to raise awareness with regard to vulnerabilities in this sector.

Detection

Given the ubiquitous vulnerabilities in existing Commercial Off-the-Shelf (COTS) software, intrusions into critical systems are inevitable for the foreseeable future. Thus, detection of these intrusions is critical if the U.S. Government and critical infrastructure owners and operators are going to be able to respond. To improve our detection capabilities, we first need to ensure that we are fully collecting, sharing, and analyzing all extant information from all relevant sources. It is often the case that intrusions can be discerned simply by collecting bits of information from various sources; conversely, if we don't collate these pieces of information for analysis, we might not detect the intrusions at all. Thus the NIPC's role in collecting information from all sources and performing analysis in itself aids the role of detection.

The NIPC is currently concentrating on developing and implementing reliable mechanisms for receiving, processing, analyzing and storing information provided by government and private sector entities. This information is being used by NIPC analysts to develop tactical and strategic warning indicators of cyber threats and attacks. The NIPC and North American Energy Reliability Council (NERC) have established an industry-based Electric Power Working Group to develop tactical warning indicators and information sharing procedures for the electric power sector. The NIPC also has developed mechanisms to share cyber incident information with both government agencies and private companies in the telecommunications sector. In the long-term, our indications and warning efforts will require participation by the Intelligence Community, DOD, the sector lead agencies, other government agencies, federal, State and local law enforcement, and the private sector owners and operators of the infrastructures.

Another initiative that will aid in the detection of network intrusions is the ``Federal Intrusion Detection Network'' (``FIDNet''), a National Security Council initiative that would be managed by the General Services Administration. Many agencies already have their own intrusion detection systems. FIDNet will enhance agencies' cyber security by linking their intrusion detection systems together so that suspicious patterns of activity can be detected and alerts issued across agencies. The goal of FIDNet is to detect intrusions in the federal civilian agencies' critical computer systems. (Contrary to recent press reports, FIDNet will not extend to private sector systems.) To do this, critical network event data will be captured and analyzed so that patterns can be established and, in the event of an attack, warnings issued. FIDNet will be the civilian agency counterpart for the automated detection system currently deployed across Department of Defense systems. FIDNet, under current plans, will consist of the following: sensors at key network nodes; a centrally managed GSA

facility, the Federal Intrusion Detection Analysis Center (FIDAC), to analyze the technical data from the nodes; and secure storage and dissemination of collected information. The NIPC will receive reports from the FIDAC when there is evidence of a possible federal crime (such as a violation of 18 U.S.C Sec. 1030). Using all-source information, the Center would then analyze intrusions and other significant incidents to implement response efforts and support and inform national security decision-makers. FIDNet-derived information would also be combined with all-source reporting available to the NIPC to produce analysis and warning products which will be distributed to government, private sector companies, and the public, as appropriate.

Response

The NIPC's and the FBI's role in response principally consists of investigating intrusions to identify the responsible party and issuing warnings to affected entities so that they can take appropriate protective steps. As discussed earlier, in the cyber world, determining what is happening during a suspected intrusion is difficult, particularly in the early stages. An incident could be a system probe to find vulnerabilities or entry points, an intrusion to steal or alter data or plant sniffers or malicious code, or an attack to disrupt or deny service. The cyber crime scene is totally different from a crime scene in the physical world in that it is dynamic--it grows, contracts, and can change shape. Determining whether an intrusion is even occurring can often be difficult in the cyber world, and usually a determination cannot be made until after an investigation is initiated. In the physical world, by contrast, one can see instantly if a building has been bombed or an airliner brought down.

Further, the tools used to perpetrate a cyber terrorist attack can be the same ones used for other cyber intrusions (simple hacking, foreign intelligence gathering, organized crime activity to steal data, etc.), making identification and attribution more difficult. The perpetrators could be teenagers, criminal hackers, electronic protestors, terrorists, foreign intelligence services, or foreign military. In order to attribute an attack, FBI Field Offices can gather information from within the United States using either criminal investigative or foreign counter-intelligence authorities, depending on the circumstances. This information is necessary not only to identify the perpetrator but also to determine the size and nature of the intrusion: how many systems are affected, what techniques are being used, and what the purpose of the intrusions is--disruption, espionage, theft of money, etc.

Relevant information also could come from the U.S. Intelligence Community (if the attack is from a foreign source), other U.S. government agency information, state and local law enforcement, private sector contacts, the media, other open sources, or foreign law enforcement contacts. The NIPC's role is to coordinate and collect this information.

On the warning side, if we determine an intrusion is imminent or underway, the Watch and Warning Unit is responsible for formulating warnings, alerts, or advisories and quickly disseminating them to all appropriate parties. If we determine an attack is underway, we can issue warnings using an array of mechanisms, and send out sanitized and

unsanitized warnings to the appropriate parties in the government and the private sector so they can take immediate protective steps. The Center has issued 22 warnings, alerts, or advisories between January 4 and September 22, 1999.

Two other NIPC initiatives are directed to improving our response capabilities. First, to respond appropriately, our field investigators need the proper training. Training FBI and other agencies' investigators is critical if we hope to keep pace with the rapidly changing technology and be able to respond quickly and effectively to computer intrusions. The NIPC has been very active in training. These training efforts will help keep us at the cutting edge of law enforcement and national security in the 21st Century. The Center provided training to 314 attendees in fiscal year 1998. In fiscal year 1999, over 383 FBI Agents, state and local law enforcement representatives, and representatives from other government agencies have taken FBI-sponsored courses on computer intrusions and network analysis, the workings of the energy and telecommunications key assets, and other relevant topics.

Second, our Key Asset Initiative (KAI) facilitates response to threats and intrusion incidents by building liaison and communication links with the owners and operators of individual companies in the critical infrastructure sectors and enabling contingency planning. The KAI began in the 1980's and focused on physical vulnerabilities to terrorism. Under the NIPC, the KAI has been reinvigorated and expanded to focus on cyber vulnerabilities as well. The KAI initially will involve determining which assets are key within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets. FBI Field Offices will be responsible for developing a list of the assets within their respective jurisdictions, while the NIPC will maintain the national database. The KAI is being developed in coordination with DOD and other agencies.

CONCLUSION

While the NIPC has accomplished much over the last year in building the first national-level operational capability to respond to cyber intrusions, much work remains. We have learned from cases that successful network investigation is highly dependent on expert investigators and analysts, with state of the art equipment and training. We have begun to build that capability both in the FBI Field Offices and at NIPC Headquarters, but we have much work ahead if we are to build our resources and capability to keep pace with the changing technology and growing threat environment and be capable of responding to several major incidents at once.

We have also demonstrated how much can be accomplished when agencies work together, share information, and coordinate their activities as much as legally permissible. But on this score, too, more can be done to achieve the interagency and public-private partnerships called for by PDD-63. We need to ensure that all relevant agencies are sharing information about threats and incidents with the NIPC and

devoting personnel and other resources to the Center so that we can continue to build a truly interagency, ``national'' center. Finally, we must work with Congress to make sure that policy makers understand the threats we face in the Information Age and what measures are necessary to secure our Nation against them. I look forward to working with the Members and Staff of this Committee to address these vitally important issues. Thank you.

Senator Kyl. It is my understanding that, with the exception of one paragraph, the draft statement that had not previously been cleared is the statement that you have submitted for the record today, is that right?

Mr. Vatis. What we brought this morning is the final statement, yes, sir.

Senator Kyl. And that statement, since Mr. Vatis did not recount in detail all of the examples of things that had been dealt with or are being dealt with, I might just reiterate, just to highlight a couple, one estimate of damage from the 80 to 100 events daily detected is, in the first two quarters of 1999, a loss or damage from these viruses over $7 billion. This is not a minor matter.

Then the other examples of foreign sources interfering with the Kosovo operation, the foreign intelligence services with information sold to the Soviet KGB, terrorist activity, the criminal groups which you have mentioned, the Phonemasters case, which I mentioned, and a variety of other situations, but there was one item that I referred to from open source material, I believe it was Newsweek magazine. Can you say anything on the record about that particular ongoing event and can you identify it by its code name?

Mr. Vatis. The article called it Moonlight Maze, and that is, in fact, our name for an investigation that we have been conducting for over a year into a series of widespread intrusions into Department of Defense, other Federal Government agency, and private sector computer networks. About the furthest I can go is to say that the intrusions appear to originate in Russia. We have been coordinating an investigation that has involved numerous Federal agencies, as well as international counterparts, but the intrusions have resulted in the taking of or the theft of unclassified, and it is important to stress that it is unclassified, but still sensitive information about essentially defense technical research matters.

Senator Kyl. Thank you very much. I think none of us underestimates the seriousness of the issue, but I think it is important that hearings like this convey to the public as much information as can possibly be conveyed about the threat so that the public will be supportive of the efforts of the government and the private sector to deal with it, and also so that they will appreciate the law enforcement tension that you identified, and I am going to get more into that in a minute, to try to put everybody's mind at ease with respect to how the investigations are proceeding and how privacy is being protected.

Mr. Tritak, let me ask you, the PDD was issued back in May 1998 and I think the 180-day time frame which mandated that the plans be developed was probably unrealistic at the time. But it has now been over a year and we still do not--well, let me ask you. A, have plans been completed, and B, if not, why not, and C, when we might expect that the initial operating capability, which was supposed to be by November 2000, will, in fact, be achieved?

Mr. Tritak. Yes, Senator. Let me say that the plan is in its final stages of interagency review and clearance. It is our strong hope that it will be issued later this month or early next month. So I think, recognizing that, as you have indicated, I think when the initial goal of 180 days was made, the complexity of the task at hand perhaps was not quite as well appreciated as it became in the course of developing it.

But let me say a couple of words about that, because I think it is important to understand that we are talking about rather an unprecedented process of engaging some 24 agencies in addressing an issue that everyone recognizes is important. How one goes about it, especially given budgetary realities, is something that is open to serious consideration and debate, sometimes very spirited debate. I think that is a good thing because this is a big issue and you want the benefit of very careful thought given by a wide range of experts within the government on this matter.

Now, when the plan does come out, it is probably best to think of it as an invitation to a dialogue rather than a final product to be embraced and accepted thumbs up/thumbs down. That is mainly because the main focus of the national plan is on the Federal Government's efforts. I think the rationale for taking this approach is if we are going to engage the private sector and ask them to support the efforts that are needed to protect our critical infrastructures, the government has to show a level of seriousness in getting its own house in order.

So what you are going to see, for the most part, in the first version is the Federal Government's initial attempt at developing a plan that it will implement and pursue in the ends and goals of PDD 63. It is hoped that once this is issued, it will be very quickly followed by a broader dialogue with private sector interest groups, particularly in the privacy area, but also members of Congress and their staffs because we cannot consider something to be a national plan without engaging the Nation in this dialogue. It affects everyone importantly.

So in answer to your question, it is coming out very soon and we are hoping that it will be, again, the later part of this month, the early part of next month.

Senator Kyl. Thank you. This is not the time to be critical. I really was simply focusing on the questions that Senator Feinstein raised at the end of her statement, and I think we all want to work constructively toward the result. I can remember former Senator Sam Nunn and I testifying about this, and I have forgotten now when that was, but clearly, he has not been around for a while. This has been going on for a

long time and we have had to prod some people within the administration for quite a while to get going here.

Again, I am not being critical of you or the people who are working hard on this. As you point out, it is a hard job. But in view of the kind of threats that have been mentioned here, I do not think we can say too often that we have got to get on with this and put these plans in place.

Just very quickly, because I do not want to take any more time here, you testified that this program would operate within legal requirements and government policy concerning privacy, civil liberties, and promoting confidence in users of the Federal/civilian computer systems, that neither the FBI nor other law enforcement entities would receive information about computer attacks and intrusions except under longstanding legal rules and where an agency determines there is sufficient indication of illegal conduct, that private entities will not be wired to the FIDNet, no private sector entity is a part of the civilian government program, and that it will be run by GSA, not the FBI. It will not monitor any private networks or e-mail traffic and confer no new authorities on any government agencies and will be fully consistent with privacy law and practice, right?

Mr. Tritak. Right.

Senator Kyl. I think that is an important point to get across to folks, that we are dealing with a very significant national security issue here, and as Senator Bennett pointed out, there will be times when it may be unclear to us but it moves into a law enforcement requirement, but that in no event will any policies or rules be changed, which obviously that is a concern of this committee, because we understand that the U.S. Constitution would prevent any inhibitions on privacy rights in any event. I just want to try to help put people's mind at ease that everyone is very cognizant of that, the people in charge of putting the plan together, some of the people in charge of oversight here, and we will continue to keep our eye on that.

Senator Feinstein.

Senator Feinstein. Thanks very much, Mr. Chairman.

Mr. Vatis, in your testimony, you mentioned, and Senator Kyl, I think, referred to it, that the DOD has reported 80 to 100 hacker attempts every day. Do you know how many of these attempts succeed?

Mr. Vatis. I do not have exact numbers, Senator, on how many succeed. There is a whole range of effects of possible attacks. Sometimes they are just pings that attempt to probe a system. Sometimes they get in successfully but then do not do anything. And sometimes they get in and then they do things, such as remove information or----

Senator Feinstein. Then let me ask you the next question, which you probably do know the answer to. What kind of damage, if any, is occurring?

Mr. Vatis. In general?

Senator Feinstein. Yes, or as specific as you feel you can.

Mr. Vatis. It depends on the case. Generally, what we see

is people looking around and sometimes taking information on the unclassified networks. There have not been many instances where damage has been done to the systems. The primary concern in most of these cases is with unauthorized, illegitimate access to information that, though unclassified, is sensitive military information.

Senator Feinstein. You said there have not been many occasions when significant damage has been done, but has some damage been done?

Mr. Vatis. I am sure there are instances where somebody has done damage. I do not have any specific recent examples to bring to you.

Senator Feinstein. You mentioned Operation Moonlight Maze. In that operation, has there been any penetration of classified systems?

Mr. Vatis. I should not get into that area in this setting.

Senator Feinstein. I would be interested, perhaps in a classified setting, if you might be able to indicate that. I think those are key questions.

Senator Kyl. Excuse me. I might mention, we had a briefing established yesterday by Dick Clark.

Senator Feinstein. I could not attend.

Senator Kyl. Well, none of us could and, therefore, it was cancelled, but we will do it. We will reschedule it when everyone can attend and we will do that.

Senator Feinstein. If we could discuss this in that briefing, I think that would be----

Senator Bennett. If I may, Senator, we have had a briefing on that in the Y2K Committee. I agree with the witness, these are classified matters, but I agree with you in pursuing them because they are very important.

Senator Feinstein. I was recently told that there are certain computer software available for free on the Internet that allows a person to install what amounts to an undetectable trap door on another person's computer. As long as that computer remains hooked up to the Internet, the hacker can then read the target's e-mails, see every password, move the mouse, erase files from the computer, and even shut it down, all without detection or recourse. I understand that some of the software is commercially available and beneficial for internal company use, but it also seems to me that some people are clearly trying to teach people how to infiltrate outside computers and do some real harm. Are you aware of this kind of software?

Mr. Vatis. Yes, we are. There are several instances of that. One recent piece of software that fit that description is something called Back Orifice 2000, which was released at the recent DeathCom hackers' conference in Las Vegas, which permits an external user to gain unauthorized access and do things to another person's system along the lines that you mentioned. This is something we are aware of. We have actually issued several advisories to both government agencies and the private sector about that particular tool. But these types of tools, hacking tools, pop up daily and there are new tools. I am sure

you will hear from Rich Pathea about more specifics on those types of things. But the one you mentioned, if I think that is the one you are referring to, is one we are very well aware of and have issued warnings on.

Senator Feinstein. Are there any commercial systems available that can pierce classified systems?

Mr. Vatis. The protection of the classified systems is mainly a matter of controlling the access. It is not that they are impenetrable, per se. Beyond that, I really do not want to get into that area of the classified systems.

Senator Feinstein. If this could be another area, Mr. Chairman, that we could discuss, because there is--and you and I have both been involved in the encryption area, and there is this strong feeling in the industry about protecting privacy, with which I think we both agree. Now, here we are with systems commercially being devised to pierce that and to sabotage that very same privacy and put these on the open market. I think that raises a very real question that what would be appropriate regulation by the government, if any, of systems that pierce the privacy and really can sabotage a system.

Do you have any suggestions as to what can be done to ensure that teenage hackers or others do not simply leave such trap doors or computer programs on the computers they penetrate?

Mr. Vatis. A lot of the security measures that we would recommend are really rather basic and it is a question of devoting sufficient resources and attention to those basic security measures. Careful perimeter security design of a network, augmented by careful personnel security policies, because oftentimes the beginning of a successful intrusion is social engineering and getting passwords or log-in information by calling up a user and pretending to be someone who forgot his password, for instance. The use of smart cards and tokens, one-time passwords, would also be a successful way to implement security, and updating virus detection software and also implementing the latest patches that are made available are all basic security practices that are too often neglected.

Senator Feinstein. Are those protections in place in all, I will not use the word highly secure systems, but all key government systems today?

Mr. Vatis. Basic security policies are in place across the government to effect that sort of security. Where the breakdown sometimes occurs is in the implementation. The Solar Sunrise case is another good example of that. The vulnerabilities that the teenagers took advantage of were ones that were known throughout the network community, the system administrator community, and, in fact, patches were available to fix those vulnerabilities. The problem was that the patches had not been implemented across the DOD systems. So the policies exist, but it is the implementation that is the difficult part.

Senator Feinstein. What about the private systems, airlines, railroads, telephones, power systems?

Mr. Vatis. The difficulty there, as Mr. Tritak referred to, is that these are privately owned systems over which the

government has very little directive authority or regulatory authority. Much of the private sector is beginning to pay more attention to security and the need to have good security practices, to spend money on effective security, because they are beginning to see that poor security will have a deleterious impact on the bottom line. But it is still a problem in the rest of the private sector of getting the decision makers, the corporate decision makers, to focus enough attention and resources on that type of security.

Senator Feinstein. Let me ask this question. Of these kinds of systems, and I am speaking about the big systems, what would you say the level today of vulnerability is, low vulnerability, medium vulnerability, or high vulnerability?

Mr. Vatis. As a general matter, I would have to say it is high. I think there are significant vulnerabilities in these critical systems that not only can be taken advantage of but are being taken advantage of. We have not seen what some people have referred to as the electronic Pearl Harbor, where somebody has used those vulnerabilities to engage in a massive destructive attack. But just the examples that we have discussed this morning should be sufficient to indicate to people and to demonstrate that these significant vulnerabilities do exist. If teenagers can gain the type of access to the types of systems that we have seen just in the last couple of years, those instances in themselves should demonstrate the level of vulnerability.

Senator Feinstein. We had one situation in San Francisco at a PG&E, it seemed to me, plant where everything got shut down. So what you are saying is, in the private sector, in terms of the civilian infrastructure, today, there is a very high vulnerability and that the private sector has not responded significantly to use available technology to quell that vulnerability?

Mr. Vatis. It is a mixed bag, but I think, in general, when we are talking about those critical infrastructures, there are significant vulnerabilities that do exist and that is one of the reasons that we have been trying to engage in information sharing about the vulnerabilities, about the threats, to make people aware in the private sector of where the vulnerabilities lie, what types they are, and also what the threats are that might take advantage of those vulnerabilities.

But again, we should not act as though the private sector does not have its act together but the government does, because I think, as Mr. Tritak said and as the next panel will get into, there are also significant vulnerabilities in the government. So I think the Nation as a whole, both the private sector and the public sector, needs to face up to this and deal with these vulnerabilities.

Senator Feinstein. Thanks very much, Mr. Chairman.

Senator Kyl. Thank you. I think particularly important is the fact you brought out that the efforts here are not invasive of privacy but rather are important in order to protect people's privacy. That is very important.

Senator Bennett.

Senator Bennett. Thank you, Mr. Chairman.

In July, you both testified before the Y2K Committee and there were no clear answers as to what cyber reconstitution was. We talked about that at that time. Can you tell me now, in the case of either a Y2K failure or an IW event, where there is an actual attack to try to shut something down, how the United States would facilitate cyber reconstitution, in other words, bring a system back up? This is for either one.

Mr. Vatis. I think my answer would still be the same as in July, which is that reconstitution of private systems, at least for the first part of the answer, the responsibility resides first and foremost with the private sector, but the assistance to the private sector is the responsibility of the lead agency under PDD 63, to provide the expertise and any assistance that we can offer. Then the consequence management for disruption, providing emergency generators, for instance, in the event of an attack on the electrical power system, would be the responsibility of FEMA.

Senator Bennett. Yes. Well, the FEMA example is the obvious one. You have a disaster, whether it is a tornado in Salt Lake City or an earthquake in California or a hurricane off the coast of Florida, and here is a government agency that steps in after the fact to try to help rebuild the essential infrastructure. I just asked the question in order to keep the issue alive, recognizing that we do not have those kinds of answers, but we need to keep focusing on this, because if somebody does succeed in shutting us down, we ought to have some sort of electronic FEMA in place that can say, all right, we were not able to prevent it, but we can reconstitute the service relatively quickly.

Senator Feinstein talked in terms of success. Just a quick editorial comment. My concern, and that is shared by a lot of the folks with whom I have spoken over this particular odyssey, has to do with people who get in undetected. Success is when you can stop it at some level. But is there a level where people have gotten in, gotten the information they want, and gotten out without our knowing it? Not to sound like a Tom Clancy novel, but the last one I read that described how a Russian submarine had tracked an American submarine without the Americans realizing it. I think there is some indication that there may be some of that, that not necessarily the teenage hackers but nation states have gotten into our computers, gotten the information they were looking for, and left, and most frighteningly, maybe left behind a trap door that would allow them to do that undetected wherever they are.

I make that point simply to underscore once again, we are living in a new world. We are living where there is no sanctuary. We are not hiding behind our oceans. Our potential enemies are, indeed, in our bowels, if you will, and it becomes very important for us to just start thinking that way as we look for remediation.

It is my experience that when you talk to people in industry about this issue, you get the same kind of response we initially got with respect to Y2K. That is, hey, it is not

really a problem and our IT people will handle it and it will all go away. We will get it under control. It was not until we got the attention of the CEO as well as the CIO that we got significant progress in industry.

When I talk to industry leaders, they all say, oh, we have firewalls. We have spent the money. We have firewalls. My sense is that these firewalls have never really been tested the way the firewalls of the Defense Department, for example, have been tested. The Defense Department is a whole lot harder than a lot of people realize. I have now spent enough time going around to Defense Department installations to discover that. But I am not sure how hard some of the private institutions are.

Do either of you have a sense of how effective the firewalls are in private industry compared to the government?

Mr. Vatis. I think it varies tremendously, whether they even have firewalls, first of all, and second of all, how good the firewalls are, and then third, whether the firewall and other security measures are actually implemented properly. But no firewall is impenetrable, and I think sometimes people have a false sense of security. As you indicated, merely from the fact that their IT guys assure them that they have a firewall, they think as a result that they are totally secure, and that is a false sense of security.

Senator Bennett. I do not want to get across the line into classified information, but let me posit this as a hypothetical. Suppose a U.S. Government red team were formed and offered to make an attempt to get into certain industry areas, just as an exercise. How do you think industry officials would react to that?

Mr. Vatis. I think some of them would actually welcome that kind of assistance in testing their systems and others might be averse to it because they would not want to know the answer.

Senator Bennett. How about government agencies outside of the Defense Department? Say, for example, the Department of Energy, that has responsibility for our nuclear weapons, was told, OK, that is wonderful that you have all of these protections. Now we are going to try to penetrate you. Do you think the Secretary of Energy should cooperate with that effort?

Mr. Vatis. Absolutely. I think red-teaming is an important part of any set of security measures because the only way to know whether your security measures are adequate is to test them. So I think that is a critical thing.

Senator Bennett. Thank you, Mr. Chairman.

Senator Kyl. Thank you. Senator Feinstein.

Senator Feinstein. Let me just thank you for being up-front and forthright with this. I think it is really important and I appreciate the fact that you speak directly. It is my understanding that at least 22 of the largest Federal agencies have significant computer weaknesses, either because they do not know how to fix the problem or because they do not realize the problem exists. The GAO report gives some examples.

In May 1999, NASA computer-based controls were successfully penetrated on several mission-critical systems. In August 1999,

serious weaknesses in DOD's information security continued to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data. I mean, that is a month ago. In July 1999, GAO reported the Department of Agriculture's national finance center had serious access control weaknesses. And in October 1999, which is now, we report that the Department of Veterans Affairs systems continue to be vulnerable to unauthorized access, and they point out one VA insurance center, 265 users who had not been authorized access had the ability to read, write, and delete information related to insurance awards.

Have these been remedied? These 22 agencies, have their weaknesses been remedied?

Mr. Vatis. I do not know the answer to that question.

Senator Feinstein. Mr. Tritak.

Mr. Tritak. I do not know the answer to that question, either.

Senator Feinstein. Our next panelist does? Good. Perhaps they can answer it. I look forward to it. Maybe that is a good segue.

Senator Kyl. Thank you very much.

We would really appreciate your responses, because as we have mentioned here, this will be just one in a continuum of hearings. We obviously will want to get a report about the timing on the completion of the plans and on the operations capability and time frames. We will want to have you come back and report that to us.

I am looking forward, Mr. Vatis, to perhaps even getting into just two or three specific kinds of cases, one attack on our defense or security infrastructure, one financial attack to steal money, and then perhaps another one, either an insider attack or a terrorist kind of attack. I think it would be very interesting to have you get into detail about--just take two or three or four case studies and walk through them and talk about the three or four different kinds of intrusion that can take place and how it does without getting into too much how-to, obviously.

I believe that, as Senator Bennett said, this does sound a little bit like Tom Clancy, but it is a reality and people are fascinated by it. If they can come to be fascinated by it, they can come to be concerned about it and then we can help Mr. Tritak and others get their job done on a timely basis.

I thank both of you for being here very much and would like to call the next witness now, Jack Brock. We will get started, and if we have to be interrupted, we will, but I would at least like to begin the testimony.

Mr. Brock, as I said, is with GAO. He is the Director of the Government-Wide and Defense Information Systems, Accounting and Information Management Division, and will testify specifically to what GAO has found with respect to government vulnerabilities and hope to be able to answer the questions that Senator Feinstein got into.

Senator Feinstein. I did not mean to jump his testimony.

STATEMENT OF JACK L. BROCK, JR., DIRECTOR, GOVERNMENT-WIDE AND DEFENSE INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE, WASHINGTON, DC; ACCOMPANIED BY JEAN L. BOLTZ

Mr. Brock. I hope so. With your permission, Mr. Chairman, I would like to have Ms. Boltz----

Senator Kyl. We welcome Jean Boltz on the panel, as well.

Mr. Brock. Thank you.

Senator Kyl. Thank you. Go ahead.

Mr. Brock. I appreciate very much, Ms. Feinstein, your summarizing the most interesting part of my statement, and you did it very effectively.

I think the first two witnesses, as well as the opening statements, Mr. Chairman, of you and Ms. Feinstein and Senator Bennett, very effectively talked about that there is a real threat, that there are real opportunities with connectivity and that these opportunities are wonderful. They offer incredible advances in the way we do business, the way we communicate, and the future opportunities are even greater and we do not want to lose that advantage. Almost ironically, though, these same opportunities offer new ways of disrupting the national infrastructure, and that is what the purpose of your hearing is today.

I want to focus primarily on the Federal portion of that. We have reported that 22 of the largest Federal agencies have significant weaknesses and our statement details several examples. We could have gone on page after page after page of examples, were it NASA, at VA, at, although we did not list it in here, the Financial Management Service, the Department of Agriculture, agencies that have billion dollar portfolios, agencies that protect the national defense, we have broken into.

In breaking into these agencies and doing our penetration testing, we could have done severe damage to the systems, we could have done severe damage to the information that was contained in those systems, and we could have denied access by the agencies to that information. We obviously did not do so, but the risk is there. The vulnerabilities are there.

To get to your point, and I will just answer your question now, have the agencies repaired these holes? Yes and no. At the individual problem level, they have taken immediate action. All of them have been very responsive. However, it is like having a bad roof on your house and you are continually having leaks and you put up a shingle here and a shingle there and pretty soon you have sort of shingled over the house but you are still having the leaks. These agencies need a whole new roof. It is not just a question of fixing the vulnerabilities we find.

When we go back to agencies--at DOD, we were there 2 years ago. We just issued our second report last month. At VA, we were there a couple of years ago. We just issued our report. These agencies had taken good strides in fixing the vulnerabilities we identified before, but there were new

vulnerabilities that cropped up.

We believe that at many agencies, computer security is a bottoms-up type of affair, that the real problem needs to be owned, as Senator Bennett said, by the top management, and if top management does not own the problem, if they do not provide the resources, if they do not assign the accountability, then computer security is more likely a catch-as-catch-can affair.

We have been looking at computer security for several years and we find the same problem every time--poor access controls, poor system controls, poor management controls, and we were just beginning to repeat ourselves. A couple years ago, we started work on what we called best practices or leading practices, where we went to a number of organizations that had good computer security programs, and almost uniformly, these organizations had one, a central point of control, someone that was clearly accountable for information security. That person was always accountable to the chief executive officer or the chief operating officer.

There was a real assessment of the risk that that organization faced in terms of defining threats, vulnerabilities, and the value of the information that the organization had. These organizations then developed policies and procedures and processes that allowed them to be responsive to those risks.

Next, they made people well aware of what their roles and responsibilities were and made sure that those were accountable for monitoring and maintaining control over the processes and applying them.

And then lastly, there was independent assessment of the organization's performance, and this is a continuous cycle. It is not a one-time thing that stops. It goes on and on and on. We think that if agencies did this, that, in fact, they could eliminate many of the weaknesses that they have right now. Our report has been endorsed by the CIO Council. It has been endorsed by many individual agencies. I think the level of effort, though, goes to endorsement and we have not seen a lot of real positive action on implementing the broad management reforms that need to take place.

I would like to talk a little bit, though, about PDD 63 and the current environment that is going on. We see this as a real opportunity, that there is now a discussion at a national level about issues that could have a significant impact, a positive impact, on the ability not only of Federal agencies, but also the ability of the entire infrastructure to provide better assurance that vulnerabilities will be closed up.

We have identified seven topics, though, that we think need to be addressed in the discussion in order for things to move forward. First of all is clearly defined roles and responsibilities. Under the current law, there are a lot of agencies that have some set of responsibilities and duties. It is not always clear what these are and it is not always clear that they are being implemented. PDD 63 has also introduced a number of new organizations and many of these organizations and processes are immature and have not found their way yet. So it

is unclear how they are going to relate and interrelate and it is unclear about what sort of impact they can have on agencies and on the private infrastructure. So it is important that as the debate unfolds, that roles and responsibilities be clearly defined, that authorities and accountability be clearly defined.

Second, we see a need for specific risk-based standards. Right now, most of the guidance is very general. For example, NIST issues guidance saying that users should be authenticated. Well, that can mean anything from a four-digit password to your thumbprint. We believe that agencies need more specific guidance on how to identify risk, how to categorize these risks, and then have standards that are tailored to addressing these risks.

We think there should be routine evaluations of agency performance that we need to measure. If you cannot measure what you are doing, if you cannot report on the success, the failures, the opportunities missed, the opportunities gained, then it is really impossible to see what the lessons learned and what you need to do. The CFO Act is a good example of this, where there are now independent audits of agencies' financial statements, and as a result of that, agencies have made incredible strides in improving their financial management operations over the past 5 years. We think similar opportunities exist with computer security.

Next, executive branch and Congressional oversight. Senator Bennett has been instrumental in the Senate in terms of providing very rigorous oversight over Y2K issues. Just as importantly, though, most of the individual committees that have oversight over individual agencies have also had hearings, and not just one hearing but multiple hearings. The same thing is true on the House side. The same thing is true in the executive branch, where the oversight over Y2K has been notably more rigorous than it has been on computer security issues.

As a result of this, many of the hurdles have been overcome by the constant pressure of the spotlight being shone on the issue, identification of things that need to be done, and solutions reached. So a continuation of that type of executive branch and Congressional oversight and leadership is important in this area, as well.

The next area is adequate technical expertise. If you do not have the right kind of people, you are not going to come up with the right kind of solutions, and this is a problem. We have an executive council of independent CIO's in the private sector. They are telling us that a system administrator that is well qualified can make about $150,000 in the private sector. That is not true in the public sector. There is inadequate training. There are just not enough people sometimes to go around. If this problem is not addressed, then regardless of the policies and procedures and the good work that goes into it, if you do not have the technical resources to carry it out, you still will not be able to reach success.

The next area is adequate funding. The most positive response we got to our publication last week on critical

infrastructure protection, comprehensive strategy control, and year 2000 experiences, we pointed out in that report that there was funding for Y2K fixes, that the funding was made available not only with the agencies directly in their budgets but also in the emergency supplemental fund, that there was a relatively good assurance that the funds would be available. That is not always true on computer security.

On the other hand, because of the relatively low level of some agencies in terms of their abilities to effectively deal with the problem, you do not also want to paper it over with money. You need to make sure that if agencies have more funds, that they are also prepared to spend them wisely.

Incident response and coordination, and again, talking about the Federal Government, there is no real requirement to report incidents. As a real matter, within some agencies, we find that even within the agency, they do not report incidents, if they are aware of it. Certainly, agencies are not uniformly reporting them to FedCIRC, housed at GSA, and as a result, opportunities are missed to learn from what agencies are experiencing, opportunities within the agency and opportunities among the agencies.

We think that if these seven issues come up for serious discussion and resolution during the discussion of the national plan and then placed on top of a renewed infrastructure within the agencies, that solutions are available to improve computer security within the government. There is no panacea. There is no magic bullet. There is no assurance that problems will be completely eliminated, but we think there is lots of opportunity for improvement.

Mr. Chairman, that concludes my statement, and Ms. Boltz and I would be happy to answer any questions you might have.

Senator Kyl. Thank you. There are other important hearings going on today, but I think what you have said here, while I know it has been in the public domain before, maybe has not been focused on, and I think it is important that I repeat just a little bit of it and have you comment on it.

You are basically saying that through your audits, the GAO audits, you found that our government--I am quoting now--``is not adequately protecting critical Federal operations and assets from computer-based attacks.'' You go on to say that the audits show that 22 of the largest Federal agencies have significant computer security weaknesses, right?

Mr. Brock. That is correct.

Senator Kyl. You further say that reports issued over the last 5 years describe persistent computer security weaknesses that place Federal operations such as national defense, law enforcement, air traffic control, and benefit payments at risk of disruption, as well as fraud and inappropriate disbursements, I think is the word, or disclosures.

Mr. Brock. Yes, sir.

Senator Kyl. Specific incidents, you mention just this year you successfully penetrated several mission-critical systems of NASA. Just in August of this year, you reported weaknesses in DOD's system that provide people the opportunity to modify,

steal, inappropriately disclose, or destroy sensitive DOD data. You talked about the fact that DOD functions, including weapons and supercomputer research, as well as others, have already been adversely affected by system attacks or fraud.

Mr. Brock. That is correct.

Senator Kyl. See, those are very important, disclosures that are important for the public to appreciate, and I do not believe that the message has gotten out yet. I am told that you have to repeat something 6 times before it takes hold. Maybe that is true in the Senate; I am not sure about the public generally. But I think it is important that the results of this GAO work be conveyed to the public in order to help generate the support for the financial systems that is needed as well as the other reforms that you pointed out can be accomplished.

Let me ask you whether you can say whether in these attacks by GAO you were able to gain access to classified information.

Mr. Brock. We were focusing our penetration test on sensitive but unclassified systems.

Senator Kyl. OK.

Mr. Brock. The last thing I ever want to see is a headline in the morning saying, ``GAO Brings Down Critical Systems.''

Senator Kyl. Yes. Why has it taken so long for PDD 63 to get off the ground? You mentioned that there has been no real action on the broad reforms that are necessary, and we heard testimony earlier that you heard about the delays of well over a year in getting this plan off the ground. Why is it taking so long?

Mr. Brock. I think there are a couple of reasons. First of all, let me say that I think the concept behind PDD-63 is long overdue. However, you are starting from an environment where there was not a lot of consensus over what needed to be done and how it should be done, and I think that part of the delay has been in building that consensus. I think part of the delay, as well, is one of the requirements of PDD 63 is for each of the agencies to develop a plan. It has taken a long time to develop those plans and it is taking a long time to get them in the kind of shape, because they are also starting from ground zero.

So part of it is trying to bring some people together that may have some different agendas. I think that is important to do that. Part of it, I am sure, is logistics, and part of it has been, I believe, the inability of some agencies to respond with the kind of material that was required by PDD 63.

Senator Kyl. Let me add just two more things. First of all, this subcommittee will continue to explore, in particular, any legislative action that might be necessary. We can generate that as an ongoing committee of the Senate. The Y2K Committee, of course, does not do that, but they point out problems and then we can take it from there. So we will continue to focus on that, and if there are any legislative suggestions that you want to bring to our attention that become apparent, or the need for which becomes apparent as a result of your auditing, I hope you will just consider this an open request to do that.

But second, I am going to quote one statement you conclude

your statement with, that weaknesses continue to surface because agencies have not implemented a management framework for overseeing information security on an agency-wide and ongoing basis. Because of that, I am going to recommend to the chairman of the Government Operations Committee, which would have a different kind of oversight jurisdiction, to review your audits very carefully, prioritize them in some way to identify those that seem most behind, and to begin bringing them in, agency by agency, to ask very specific and very hard questions using the information from your audits to bring to light some of the deficiencies. Obviously, the goal here is not to point fingers, but as you pointed out, to get on with the fixes that have to be put into place.

Do you have any other comment about what we could do to help advance this all, in addition, of course, to helping to provide the resources that you identified earlier?

Mr. Brock. I think the constant spotlight, the questions, the suggestion you had for the committee to bring the individual agencies up, I mean, that imposes a level of accountability that forces action. It forces the top management within those agencies to say, here is an issue that Congress is interested in. I need to elevate my own interest. As I said, that was very successful in Y2K and I think it can be successful in computer security, as well.

Senator Kyl. Whether we do that in this subcommittee or if another full committee takes that oversight, we will expect to maybe check back with you in a few months, maybe sometime mid-year next year and have you give an honest, straightforward, unvarnished evaluation of how our government agencies are doing.

Mr. Brock. We will do so, sir.

Senator Kyl. Thank you. Senator Feinstein.

Senator Feinstein. Thanks, Mr. Chairman. You know, Mr. Brock, first of all, again, your report is very straightforward and I appreciate that very much. But we have all heard the same adage, you cannot squeeze blood out of a turnip. In many respects, the Federal Government is a turnip in this respect. You pointed out the differential in salaries. The private sector goes out, they get the most experienced personnel, their cutting-edge software, all the rest. I question whether we really have the expertise to do what is necessary.

I read your conclusions and your suggestions in your report, but the one thing where this is really lacking is how do you get that kind of cutting-edge technical knowledge that departments can go to and say, here, I know we have a problem. Do something about it. It seems to me we lack that. Now, whether it can be contracted out for in the private sector, whether the government has to put together some specific area and really bring together the brightest and the best across the nation to do this, I do not know.

But it seems to me that you can go to someone and say, look, you have got a big problem, and they can look at it and they may not even know how to remedy it or even have the people that can make the suggestions that were adequate. You spoke

about a new roof. I do not think you are going to get a new roof unless we can reach out in an unprecedented way.

Mr. Brock. I agree with you, Senator. There are sort of two aspects of that. One of the things that I believe that the national plan is contemplating on proposing are initiatives in terms of increasing skills and abilities, sponsoring more research and development in the area, training people, providing opportunities. People have been looking at salary differentials and ways of addressing that.

So looking at ways of bringing on skills, either by improving the skills on board or attracting new people, that is one issue. Contracting out, under proper controls, is an issue. Many of the weaknesses that we identified, though, are almost no cost.

When we go into agencies, for example--and these are real examples--and we find the schematic for their network topology on the website and we find on another website an open discussion of the weaknesses they have over some of their controls, it is like a bank saying, here is our building plan and here is our guard schedule and here are the guards that have bullets and here are the guards that do not. I mean, there are some basics like that that just require basic attention.

The other big area that is really, again, very basic is that many of our penetration tests are done through password guessing. We have these programs that just generate password after password after password and people are very lax in changing their passwords. They use overly simplistic passwords. This is one of the reasons we were calling for different standards for risk. For some types of information, a simple four- or five- or six-digit password probably is not enough. You need another level of protection.

So there are a lot of basic things, and some agencies have made remarkable progress in terms of addressing this within more of a comprehensive management perspective, where they are improving their information management across the board.

For example, when we have looked at controls at the Federal Reserve, they are very well done. They also have a very good Y2K program. They also have a very good information management program.

We have had some negative reports about IRS and its computer security. Recent reports have indicated they have been making real progress, and also, and I do not think it is coincidental, we have also noted that they made real progress in the way they manage their big systems development efforts, as well.

So management attention is the most critical factor, but I would agree with you that providing the availability of resources is a thorny issue and it may be one of these areas, Mr. Chairman, where some sort of legislative alternatives may need to be looked at.

Senator Feinstein. In your report, you mention that the examples that I mentioned and Senator Kyl went over more thoroughly are just examples of weaknesses. I would like to ask for the full list of weaknesses that you found.

Then second, I would like to ask you to go back in one month and repeat this and see if those weaknesses have been remedied. I will bet you they have not. I will bet you 25 cents they have not. That will be my request, and I will put that in writing to you, as well. But I would like to see the full list rather than just the examples, if I might, of the 22 departments.

Mr. Brock. OK. We can provide you with an overview of each of the 22 and details to support them, as well.

Senator Feinstein. Thank you very much. Thanks, Mr. Chairman.

Senator Kyl. Senator Feinstein, by the way, I will see your bet and raise you, but we will not convey it on the Internet. How is that?

Senator Feinstein. All right.

Senator Kyl. We probably should consider writing a letter to the President and perhaps the Director of the OMB to encourage them as they begin thinking about the new budget that they will be preparing for submission to the Congress next year, that they be very alert to the requests of the different agencies for the financial resources to accomplish all of these objectives so that it is not a matter of after the fact, that they are all focusing on their needs early on, they put those needs down, and the President is fully cognizant of them when he submits his budget to us.

Senator Feinstein. May I make one suggestion?

Senator Kyl. Absolutely.

Senator Feinstein. The prior speakers brought out that there was no requirement to report incidents. There should be a requirement to report incidents.

Senator Kyl. Mr. Brock, you alluded to that, as well. Do these agencies just not have an interagency protocol?

Mr. Brock. It is really unclear to me whether it is a matter of choice that they do not report or just a simple matter of omission. But most of them, or many of them, do not report incidents. Jean, do you have anything to add to that?

Ms. Boltz. Yes. In many cases, there is really not a commonly accepted definition of what an incident is. It can be just a probe, it can be an attack, an actual intrusion, which may or may not cause damage. So there are really no rules about what to report to whom and to when.

Senator Kyl. I agree with Senator Feinstein. This is the kind of thing where there has got to be a consistent policy, and if it cannot be done through the plan--I think the first thing would be to see if we can get them to put that in the plan for sure. If not, then legislation would be perhaps appropriate.

But as Senator Bennett has pointed out before, come January 1, who is to know what it is? The computer goes down. Well, was it because of Y2K? Was it because somebody was taking advantage of Y2K? Was it because there is just an effort to disrupt, or maybe was that the result of something more intrusive? So you cannot know for sure, and that is why, what I think Senator Feinstein's point is, all of these incidents need to be

reported and then we can sort out later what the problem is.
    Senator Feinstein. Could we write a letter formally from us to Mr. Tritak and ask that this be included in the plan?
    Senator Kyl. I think that is a good suggestion.
    Senator Feinstein. And we could put some specifics into that request.
    Senator Kyl. And we might even call upon Mr. Brock and Ms. Boltz to help us formulate that.
    Senator Feinstein. Yes.
    Senator Kyl. I really appreciate your being here today.
    [The prepared statement of Mr. Brock follows:]

    [GRAPHIC] [TIFF OMITTED] T8563.001

    [GRAPHIC] [TIFF OMITTED] T8563.002

    [GRAPHIC] [TIFF OMITTED] T8563.003

    [GRAPHIC] [TIFF OMITTED] T8563.004

    [GRAPHIC] [TIFF OMITTED] T8563.005

    [GRAPHIC] [TIFF OMITTED] T8563.006

    [GRAPHIC] [TIFF OMITTED] T8563.007

    [GRAPHIC] [TIFF OMITTED] T8563.008

    [GRAPHIC] [TIFF OMITTED] T8563.009

    [GRAPHIC] [TIFF OMITTED] T8563.010

    [GRAPHIC] [TIFF OMITTED] T8563.011

    [GRAPHIC] [TIFF OMITTED] T8563.012

    Senator Kyl. I also want to note that Mr. Richard Schaeffer, Director of Infrastructure and Information Assurance, Office of the Assistant Secretary of Defense, has submitted a written statement which will be included in the record. His statement comments on DOD's role and responsibility relative to the PDD 63 and the national plan.
    [The prepared statement of Mr. Schaeffer follows:]

PREPARED STATEMENT OF RICHARD C. SCHAEFFER, JR., DIRECTOR, INFRASTRUCTURE AND INFORMATION ASSURANCE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

INTRODUCTION

    Information Superiority is essential to our capability to meet the challenges of the 21st Century. It is a key enabler of Joint Vision 2010 and its four fundamental operational concepts of dominant maneuver, precision engagement, full dimensional protection and focused

logistics. This is because each of these concepts demands that we obtain, process, distribute and protect critical information in a timely manner, while preventing our adversaries from doing the same. Without Information Superiority we will, very simply, not be able to achieve the goals established by the Department in Joint Vision 2010.

Information technology has provided us with a means to gain a military advantage over our adversaries while actually reducing our force structure. These technologies have made precision strike and focused logistics possible. They allow us to attack targets surgically with fewer munitions (albeit more expensive ones), and manage our logistics requirements more efficiently so we can move forces much farther and faster--and sustain them--than we have ever been able to do before. Similarly, information systems are essential to the situational awareness needed to achieve dominant maneuver and full dimensional protection.

But our dependence on these systems, and their presence in every aspect of our operations, has made us very vulnerable should they be disrupted. The same technologies we can use to such advantage are becoming available to our adversaries. And because they are relatively inexpensive and accessible, the range of adversaries that potentially can cause great disruption has broadened considerably.

We no longer have the luxury of focusing our defense, as we once did, mainly on our peer competitors. We now have to establish defenses that will defeat attacks by major adversaries as well as by the terrorist, hacker, and disenchanted insider--and the latter is a significant challenge. In the past much of our defensive efforts focused on protecting our offensive capabilities. Now we also have to protect an extensive DOD information infrastructure--virtually all of which depend on commercial communications networks--as well as the other critical Defense infrastructures it supports. We simply cannot conduct and sustain offensive operations without these critical infrastructures.

I am not especially concerned about our ability to develop and employ the information technologies needed to achieve the strike, maneuver, and other offensive goals of Joint Vision 2010, I am very concerned about our ability to defend the information systems that make actual offensive operations possible. Not too long ago we focused primarily on the ``confidentiality'' aspects of our information systems (can we keep something secret). Today, we must address a much broader concept that we call `Information Assurance.' This includes not only confidentiality of information, but also the integrity of the data bases from which it's drawn, the availability of the infrastructure to deliver the message, our ability to identify and authenticate those who are using our networks, and non-repudiation features to keep people from reneging on electronic contracts. These five factors: confidentiality, integrity, availability, identification and authentication, and non-repudiation constitute information assurance or IA.

Over the past two years, we have initiated a number of efforts to improve the overall information assurance posture of the Department. We established a Defense-wide Information Assurance Program (DIAP) to bring a comprehensive IA approach to this almost overwhelming challenge of building and sustaining a secure information infrastructure. Since 1997 we have conducted a number of exercises, and experienced real

world events, that have emphasized to all of us in DOD that our information systems are interconnected, and hence interdependent. This means that we conduct our daily operations in a shared-risk environment, underscoring the need for all organizations connecting to a network to thoroughly understand the risks that exist prior to operating in that environment. Each organization must know in advance whether they can accept, manage, or adequately mitigate risks that have been accepted by others before connecting to a network.

ELIGIBLE RECEIVER, in June 1997, was the first large-scale exercise designed to test our ability to respond to an attack on our information infrastructure. Designed to test DOD planning and crisis-action capabilities, it also evaluated our ability to work with other branches of government to respond to an attack on our National Infrastructures.

ELIGIBLE RECEIVER revealed significant vulnerabilities in our information systems and the interdependence of the defense and national information infrastructures. It showed that we had little capability to detect or assess cyber attacks and that our ``indications and warning'' process for cyber events was totally inadequate.

A few months later, in early 1998, we experienced a series of attacks that targeted DOD network Domain Name Servers, exploiting a well-known vulnerability in the Solaris Operating System. Known as SOLAR SUNRISE, these attacks were widespread, systematic and showed a pattern that indicated they might be the preparation for a coordinated attack on the Defense Information Infrastructure. The attacks targeted key parts of Defense Networks at a time we were preparing for possible military operations in Southwest Asia.

SOLAR SUNRISE validated the findings from ELIGIBLE RECEIVER and helped focus the legal issues surrounding cyber attacks. Because of the world situation, it was a high interest incident that significantly increased pressure for a quick response. It also validated the need to establish a standing response team. The ELIGIBLE RECEIVER/SOLAR SUNRISE experience resulted in a number of defensive actions being taken. Specifically, we have:

- Increased our situational awareness by establishing a 24-hour watch.
- Established positive control over the identification and repair of information systems at risk--SOLAR SUNRISE could have been prevented had available patches been in place in certain computer operating systems!
- Installed intrusion detection systems on key system nodes.
- Expanded computer emergency response teams to perform alerts, critical triage and repair.
- Developed contingency plans to mitigate the degradation or loss of networks.
- Improved our ability to analyze data rapidly and assess attacks.
- Established a close working relationship with the National Infrastructure Protection Center (NIPC), teaming with law enforcement agencies and developed procedures to share information with the private sector.
- Increased ``red team'' exercises to test our systems and improve our operational readiness.

Dependence on interconnected information systems and networks will only increase as we move into the 21st Century and towards Joint Vision 2010. We cannot eliminate this ``networked dependence,'' so we have to meet the challenges of Computer Network Defense, even as we change our systems to make them less susceptible to attack. Defending a computer network is a significant challenge and the challenge is increasing daily. Actually, it is a set of very significant technical challenges and associated legal and social issues. There are significant technical problems with characterizing and attributing attacks in complex networks that have no real borders. And as we develop technical solutions, we inevitably find ourselves immersed in a host of policy and legal issues--law enforcement versus national security interests, domestic versus foreign intelligence--while trying to work significant operational problems requiring the most urgent attention.

To address the operational response problem in a coherent and integrated manner, the DOD activated a Joint Task Force for Computer Network Defense (JTF-CND). Established in December 1998, it is directly responsible to the Secretary of Defense. The Joint Task Force is, in conjunction with the CINC's, Services and Agencies, responsible for coordinating and directing the defense of DOD computer systems and computer networks. Its mission includes the coordination of DOD defensive actions with non-DOD government agencies and appropriate private organizations. This is a major first step in restructuring the Command and Control regime in the Department to address the crucial importance of computer network defense in both our war fighting and business operations. The task force is based in Washington to provide interagency access and leverage established relationships with the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), and the National Security Agency (NSA). It provides a single, accessible DOD point of contact with the NIPC. And it is co-located with the Defense Information Systems Agency (DISA) so that it can leverage their technical and operational capabilities: their network management center, an established 24 hour operations center, and regional operations centers with CINC liaison. This co-location also facilitates coordination with the National Communications System. As of October 1, 1999, the United States Space Command was assigned responsibility for computer network defense (CND), with JTF-CND reporting directly to this unified command.

It is important to understand that we will always have to deal with a network of interconnected and interdependent information infrastructures that serve an ever-expanding set of interrelated communities. We cannot avoid this global interaction. And we, DOD and the U.S. Government, will have relatively little effect on its evolution. We must take advantage of it, understand its perils, and design an appropriate level of security into our systems and procedures. We have to learn to adapt our security practices to the evolving global environment.

At the same time we must be ever vigilant to a world that is an increasingly dangerous place. As we've improved our ability to monitor network activities, the number of probes, intrusions, and cyber events we can observe continues to increase. We are now detecting 80 to 100 events daily. Of these approximately 10 each day require detailed investigation. Such investigations are carried out by many of the same people we rely on to keep our networks operational, so there are limits

on the resources we have to work with.

We also must recognize that the interconnected nature of the information infrastructure, and the increasing availability and sophistication of hacker tools, places at risk immediately any information that is not properly secured. We are increasingly concerned about those who have legitimate access to our networks--the trusted insider. This is consistent with industry experience, which reports significant losses from disgruntled or dishonest employees.

We have taken significant steps to increase our internal security and security awareness, but again, vigilance is the watchword. Internet exploitation operations can be executed remotely, from any country. They can be completely anonymous, done in real time and automatically. There are extraordinary resources available to the data ``miner.'' Our own ``red team'' assessment last year of DOD information available on the Internet revealed some very sensitive material. We recently completed a major examination of all the information the Department has on its web pages and have instituted stringent procedures to insure that classified or sensitive material, alone or in aggregate, is not inadvertently accessible.

The Secretary has also instituted a policy to insure that every individual in the DOD with access to Top Secret or a specially controlled access category or compartment make an oral attestation that they will conform to the conditions and responsibilities imposed by that access. We are using this as a means to reinforce to DOD personnel the significance of the responsibilities associated with access to this information.

We also recognize that our dependence on the information infrastructure extends to our other critical infrastructures as well. We have reorganized within OSD to bring information assurance and critical infrastructure protection together under a single Director. We have developed, and are now implementing, our Critical Infrastructure Protection plan. The Defense Department is serious about protecting its critical infrastructures. We have provided a comprehensive chapter to the national plan outlining how DOD will meet our defense mission (e.g. facilities, equipment), determining the critical assets, identifying their associated vulnerabilities, recognizing interdependencies and taking measures to protect them.

I would like to outline the two major concepts on how Critical Infrastructure Protection (CIP) will be addressed within and outside DOD.

To examine critical infrastructure (CI) issues within DOD, we will have representatives (some full time, some part time) from each of the defense infrastructure sectors--financial; transportation; public works; Defense Information Infrastructure/Command, Control, & Communications (DII/C3); Intelligence, Sensors, & Reconnaissance (ISR); health affairs; personnel; emergency preparedness; space; and logistics--that will work together to discuss common infrastructure concerns. They will identify critical nodes and networks, nationally and internationally, that the DOD depends upon to execute successful military operations. They will assess the vulnerability of such nodes and networks to physical and/or cyber attack and make recommendations to enhance their security. The infrastructure providers--the private sector--are indispensable in our execution of military operations. This brings me to my second point--how we reach outside DOD.

PDD 63 calls for a partnership with the private sector. Along with others in government, we are exploring with industry the best concepts on how we share or ``partner'' information with the private sector. Private sector involvement is crucial throughout the continuum of the Defense infrastructure, but we are working with industry to determine government and private sector companies will exchange information (e.g. classified, business confidential) and the means to which it should be shared, documented and updated routinely. At the DOD installation level, we are exploring information-sharing concepts on two fronts. First, we need to ensure that the government and private sector representatives (e.g. the installation commander and staff with the local railroad owner)--our first line defenders--jointly respond to the needs identified in the planning assessments. Second, these government and private sector representatives will need to work with state, local, and county governments as to determining what their installations need in order to support their missions. Our goal is the establishment of an information-sharing model that allows for a continuous and credible information flow from the installation level to senior levels in government to include the National Information Protection Center (NIPC).

So where do we go from here? What is the way ahead? There is no simple or single solution. Our strategy is based on a multidimensional approach. We must have trained and disciplined personnel. We must improve our operations. And we must be innovative technologically. We have to recognize that information technology is vitally important to all the DOD critical infrastructures. And we must implement this strategy through a comprehensive, coherent, and integrated Defense-wide infrastructure and information assurance program.

Some steps we are taking include:

- Employing a defense in depth security model and changing our basic approach to network architecture. A major effort is underway to fundamentally restructure the Defense Information Infrastructure into a Global Networked Information Enterprise (GNIE)--a new concept of how the Department will meet its information needs.
- Moving toward a robust, DOD Public Key Infrastructure (PKI) that can bring public key cryptography to bear to help provide the required range of assurance and data integrity services as well as permitting segregation of the networks into communities of interest. This will allow us to limit the extent of the damage an intruder can inflict.
- Increasing our deployment of more sophisticated intrusion detection and monitoring technology.
- Continuing to build strategic partnerships with industry to foster an open security framework and development of security enabled products.
- Investing our R&D dollars in developing highly assured products and systems and for real-time monitoring, data collection, analysis and visualization.

In addition, the JTF-CND is working toward full operational capability (FOC) and we are expanding our CINC, Service and Agency Computer Emergency Response Teams. We are instituting a real-time

network monitoring and reporting structure. We have established positive control through our Information Assurance Vulnerability Alert or IAVA process. We are establishing a continuous vulnerability analysis and assessment program, and are increasing our red team assessment capability. We have made significant improvements in our ability to perform long-term trend analysis, thereby identifying certain types of sophisticated attacks.

We are increasing our efforts to promote information assurance training and awareness. We are looking closely at certification and retention issues for personnel performing key functions--the system administrators and system maintainers. And we are examining an expanded use of military reserves.

Substantial progress has been made, but we must always think of it as a journey, not a destination. As new technology is created, new attacks will be developed, and new countermeasures must be adopted. There is a lot more that has to be done in virtually every area that I've mentioned today. But only by recognizing this challenge, and facing it head on, can we realize the military potential afforded by achieving Information Superiority.

Senator Kyl. I invite anyone else who would like to submit a statement for this record to do so. One of the best things, I think, we can do is to make the record here and then get that out to the public.

I appreciate the work that you are doing with GAO. Keep it up. We will be calling upon you again.

If there is not anything further, then this hearing will be adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]