S. HRG. 107–366

IMPROVING OUR ABILITY TO FIGHT CYBERCRIME: OVERSIGHT OF THE NATIONAL INFRASTRUCTURE PROTECTION CENTER

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JULY 25, 2001

Serial No. J–107–22

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
78–529 DTP WASHINGTON : 2002

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah
JOSEPH R. BIDEN, JR., Delaware	STROM THURMOND, South Carolina
HERBERT KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RUSSELL D. FEINGOLD, Wisconsin	JON KYL, Arizona
CHARLES E. SCHUMER, New York	MIKE DEWINE, Ohio
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
MARIA CANTWELL, Washington	SAM BROWNBACK, Kansas
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

DIANNE FEINSTEIN, California, *Chairperson*

JOSEPH R. BIDEN, JR., Delaware	JON KYL, Arizona
HERBERT KOHL, Wisconsin	MIKE DEWINE, Ohio
MARIA CANTWELL, Washington	JEFF SESSIONS, Alabama
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

DAVID HANTMAN, *Majority Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

IMPROVING OUR ABILITY TO FIGHT CYBERCRIME: OVERSIGHT OF THE NATIONAL INFRASTRUCTURE PROTECTION CENTER

WEDNESDAY, JULY 25, 2001

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:07 p.m., in room SD–628, Dirksen Senate Office Building, Hon, Dianne Feinstein, Chairman of the Subcommittee, presiding.

Present: Senators Feinstein and Kyl.

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

Chairperson FEINSTEIN. I would like to begin this hearing. Senator Kyl, who is the ranking member, is detained and hopefully will be here by about 2:30. At 2:15, we are scheduled to have a vote on the floor. So in order not to interrupt your testimony, what I would like to do right now is just quickly make my opening remarks and then go down and we will vote, and then come back and take our first panel.

Senator Kyl has joined us. I am delighted. He was the Chairman of this Subcommittee for a substantial period of time, and I found I really enjoyed worked with him and so we are really co-chairs rather than Chairman and ranking member.

This hearing will be on a GAO report, General Accounting Office report, on the National Infrastructure Protection Center, or NIPC—that is a wonderful Washington acronym—as it is called for short. NIPC is the leading Government body that combats cyber crime and cyber terrorism. So this Subcommittee hearing will actually cover all three parts of the Subcommittee's name—Technology, Terrorism, and Government Information.

NIPC, which was founded only a few years ago, has a broad mission to prevent, to warn against, to analyze, and to respond to cyber attacks. However, many experts, both within and without Government and the private sector, have suggested that NIPC has not fulfilled its mission. Critics have argued that it has done a poor job at analyzing and warning against cyber threats and attacks. For example, some have said that NIPC's efforts to provide warnings about the May 2000 I Love You virus and the February 2000

distributed denial of service attacks on major Internet sites were slow and inadequate.

Second, while NIPC was intended to be an interagency organization, critics have contended that the FBI has dominated the NIPC and has done a poor job coordinating with other Federal agencies in fighting cyber crime. I am not saying I necessarily believe these things. I am saying what the critics have said.

Third, critics have suggested that NIPC has not done a good at ensuring information-sharing between it and private sector and Government entities. For example, NIPC has established a two-way information-sharing partnership with only one private organization, and that is the Information Sharing and Analysis Center, or ISAC, for the electric power industry.

So that is why Senator Kyl, Senator Grassley and I asked GAO to take a look at NIPC's operations and report back its findings and recommendations. Their report, which is right here, generally confirms problems identified by the critics of NIPC.

First, the report finds that, while NIPC has issued many analyses of individual incidents, it hasn't done a good job at developing strategic analysis of threat and vulnerability data. This is because of NIPC's failure to adopt a methodology to analyze strategic cyber threats, lack of adequate staff expertise, and an absence of sufficient industry-specific data on vulnerabilities. The result has been confusion about NIPC's role and responsibilities.

The report also finds that the NIPC has not done enough to establish information-sharing and cooperative relationships with the private sector and other Government agencies.

Now, the report points out a number of things that it thinks NIPC should do, and I very much welcome the witnesses' comments on these: create procedures to ensure more information-sharing with ISACs; make more progress in developing a data base of the most important components of the Nation's critical infrastructures, the Key Asset Initiative; develop better relationships with the Defense Department and law enforcement and civilian agencies.

The report also concludes that NIPC has generally done good investigative field work. However, it points out they still need additional resources and new procedures to ensure that information flows more efficiently from the field to NIPC.

So I am very pleased that the NIPC has taken the GAO's investigation very seriously, and I am also very pleased that it shows every intention of improving its operation. In fact, the NIPC made several improvements during the GAO audit itself. One example: until recently, NIPC had not done much to recruit companies to its InfraGard program, a voluntary information-sharing network for private companies. However, in just the last 6 months, NIPC has tripled the number of InfraGard members.

So I look forward to hearing the testimony from witnesses. I think both Senator Kyl and I think this is a really important vulnerability in our entire national infrastructure, and we would like to do whatever we can to see that it is improved.

So now I will turn for his opening comments to my co-chairman, Senator Kyl.

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

Senator KYL. Well, thank you, Senator Feinstein. It is nice of you to refer to me in that fashion.

I now realize what a challenge Senator Feinstein had when I was the Chairman and she would follow me after I had laid out the whole subject of the hearing, which she has just done very nicely, I might add. So I will put my statement in the record and just add a couple of comments clearly to note the fact that this hearing does give us an opportunity to focus on what Congress can do to assist the NIPC in carrying out its mission.

The Attorney General recently called computer security one of the Nation's top problems, and announced that the administration is creating nine special units to prosecute hacking and copyright violations—just one of the problems we face. He cited a report by PricewaterhouseCoopers that businesses spent $300 billion combatting hackers and computer viruses last year. Think about that, just businesses, $300 billion in unproductive spending, just defensive against hacking and viruses last year. It is obviously a huge problem.

I think the American public is only aware of a minuscule number of the viruses that have attacked just even in the recent past. The Michelangelo virus, the Melissa virus, and the I Love You virus were, I think, fairly well known, but there are others.

Just this past Thursday, a newly discovered virus called Lion worm has been discovered by researchers. It is a self-spreading program that attacks a common software used by machines that drive the Internet. It will gather encrypted passwords that can be used to gain root access to systems. This access gives the hacker complete control of the system and the information on it. It is a frightening thought to imagine the damage that could be done if someone gained control of systems that serve our communications, financial, transportation, electrical, or defense systems in our country.

The cyber war being waged against America's infrastructure if not limited to hackers seeking the thrill of the game of disrupting computer systems. It is being waged as well by criminal groups, by foreign intelligence services, insider threats from disgruntled employees, and even politically motivated groups.

It is important to remember that although the Federal Government plays an important role in protecting this country's critical infrastructure, it can't do it alone; it has got to have the cooperation of the private sector. The private sector, remember, controls about 95 percent of the infrastructure on which the country depends.

It is crucial that Congress assist the private sector and Government agencies in fostering an environment in which information is shared quickly and fully between the two. One of the things I am going to be interested in is whether people in the private sector believe that we need to do more in certain areas, for example, in the area of the Freedom of Information Act to ensure that the private sector can give Government sensitive and important information in a timely way without the possibility that that information would

then later be made public in a way that is detrimental to the industry or business involved.

So I look forward to hearing from all of our witnesses, both Government and private sector, on how we can assist them. I am very pleased that Senator Feinstein has given us the opportunity to review the progress that NIPC has made since its inception, especially with respect to the criticisms and compliments both contained in the GAO report.

So thank you, Senator Feinstein, and I thank the witnesses.

[The prepared statement of Senator Kyl follows:]

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

Then you Senator Feinstein.

Thank you for convening this very important hearing on the National Infrastructure Protection Center. This Subcommittee originally scheduled a hearing to correspond with the release of the General Accounting Office's report on May 22nd of this year. Unfortunately, series of votes on the Senate floor on that day required that last minute cancellation of the hearing. I stated that the hearing would be rescheduled and I am pleased that Senator Feinstein, who chairs this Subcommittee, has decided to hold this hearing. We both believe that this is a vitally important issue to the welfare and safety of our nation.

In 1998, the President issued Presidential Decision Directive (PPD) 63 that established the National Infrastructure Protection Center (NIPC) to protect the nation's critical computer-dependent infrastructures from computer-based attacks and disruptions. The NIPC was given the job of providing an analysis of threats, vulnerability, and attacks; issue warnings on threats and attacks; coordinate the government's response to cyber incidents; provide law enforcement support; and promote ties with the private sector to facilitate the sharing of information. This hearing provides the opportunity to examine how effectively the NIPC in accomplishing its mission.

The Bush Administration has already emphasized the importance of cyber security and the protection of America's critical infrastructure. The President and his staff are working on a comprehensive plan that is scheduled to be released later this year on the nation's critical infrastructure.

Attorney General Ashcroft recently called computer security one of the nation's top problems and announced that the Administration is creating nine special units to prosecute hacking and copyright violations. General Ashcroft cited a report conducted by PriceWaterhouseCoopers that businesses spent $300 billion combating hackers and computer viruses last year. Clearly, it's a huge problem, and getting bigger every day.

The American public is aware of only a minuscule number of viruses that have struck in the recent past: Michelangelo, Melissa, and the ILOVEYOU viruses. Just this past Thursday, a newly discovered virus called "Lion" worm has been discovered by researchers. This is a self-spreading program that attacks a common software used by machines that drive the internet. This program will gather encrypted passwords that can be used to gain "root" access to systems. This access gives the hacker complete control of the system and the information on it. It is a frightening thought to imagine the damage that could be done if someone gained control of systems that serve our communication, financial, transportation, electrical, or defense systems.

The cyber war being waged against American's infrastructure is not limited to hackers seeking the challenge or thrill of disrupting computer systems. The assault is being waged by criminal groups, foreign intelligence services, insider threats from disgruntled employees, and politically motivated groups.

It is important to remember that, although the Federal government plays an important role in protecting this country's critical infrastructure, it cannot be accomplished without the assistance of the private sector. The private sector controls approximately 95% of the infrastructure upon which our country depends.

It is crucial that the Congress assist the private sector and government agencies in fostering an environment in which information is shared quickly and fully between the two.

I look forward to hearing from both our government and private sector witnesses on how we can assist them. I am glad that Senator Feinstein has given us the opportunity to review the progress the NIPC has made since its inception and more

and more importantly, what changes have occurred as a result of the criticisms in the GAO report.

Once again, I thank the Senator from California.

Chairperson FEINSTEIN. Thank you very much, Senator Kyl.

Since the vote hasn't been announced, let's begin this panel and then we can go, say, 15 minutes after you hear the long buzzer. Then, if that is agreeable, we will go down and vote and come right back.

The first panel is comprised of Mr. Ron Dick, who is the Director of the National Infrastructure Protection Center; Mr. Robert Dacey, who is the Director of Information Security Issues of the GAO, the General Accounting Office; Ms. Sallie McDonald, Assistant Commissioner, Office of Information Assurance and Critical Infrastructure Protection at the General Services Administration; and Mr. James Savage, Jr., Deputy Special Agent-in-Charge of the Financial Crimes Division of the Secret Service.

Welcome, witnesses, and, Mr. Dick, if we could begin with you. Once again, I am going to put a 5-minute limit on witnesses so that, because it is just the two of us, we can have a little more dialog between us.

So, Mr. Dick, please begin.

STATEMENT OF RONALD L. DICK, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.

Mr. DICK. Well, thank you very much, Madam Chairman, Ranking Member Kyl. Thank you for inviting me here today to testify about the GAO review of the National Infrastructure Protection Center.

Our work here is vitally important, and holding this hearing once again demonstrates your personal commitment to improving the security of our infrastructures and the committee's leadership on this issue in Congress.

The NIPC was created in 1998 to deal with the very complex problem of critical infrastructure protection. We started 3 years ago with no dedicated staff. As one of my colleagues put it, we had to build the plane as we flew it. But we have come far in just a few years.

As you rightly pointed out, our InfraGard initiative is now over 1,600 members, with an increase since January of over 1,000 members. I had the honor here recently on behalf of InfraGard to receive the 2001 World Safe Internet Safety Award from the Safe America Foundation in May of 2000.

We are actively exchanging information with private sector companies, information sharing and analysis centers, and members of InfraGard. Companies have found that there is value in exchanging information with the NIPC, that we can safeguard their information and provide useful information in return.

Our watch center functions around the clock with connectivity to FedCIRC; Sallie McDonald, one of the panelists here, is an integral partner with the NIPC. The National Security Incident Response Center at NSA, the Joint Task Force for Computer Operations at the Department of Defense, the anti-virus community, and the backbone providers are all partners of ours, and I am going to de-

scribe a particular incident that occurred here recently where all of those things came together for a successful resolution.

The watch has issued over 98 warnings since our inception. These warning products help systems administrators protect their computer systems before things happen. We issued warnings on, for example, the Leaves worm in June of this year, e-mail script vulnerabilities, acts of hacktivism, the Brown Orifice warning, and PGP vulnerability. All of these warnings went out prior to any widespread attacks.

Let me cite one advisory that shows, as I said, what the Center is really all about. Our advisory on e-commerce vulnerabilities combined information derived from law enforcement, intelligence, and open sources. It was coordinated with our Federal partners and with three of the ISACs. It had the desired result.

The Financial Services ISAC estimated that our warning and press conference on e-commerce vulnerabilities helped thwart 1,600 attempted intrusions on the first day following the warning. Alan Paller, who heads the Systems Administrators and Network Security Institute, which represents over 100,000 information security professionals, congratulated us for our extraordinary contribution to Internet security in sharing information on Russian and Ukrainian extortions. He said, "It was extraordinary because it detailed the level of the threat and at the same time provided forensic information that allows the community to test and fix their systems."

Our analytical products are reaching the right audiences. For example, an official with a major bank information security office told us that our "vulnerability alerts publication is a valuable service. We incorporate these with other alerts and distribute [them] throughout the...enterprise."

As you mentioned, our investigations are continuing successfully. We currently have over 1,200 of them, both domestically and internationally.

On issues of national concern, we have established four strategic directions for our capabilities growth through 2005, those being prediction, prevention, detection and mitigation. None of these are new concepts, but the NIPC will renew its focus on each of them in order to strengthen our strategic analysis capabilities.

The recent events involving the Leaves and IDA Code Red worms are good examples of the NIPC's success and progress since the GAO study. We are working well with the National Security Council and our partner agencies to disseminate information and coordinate strategic efforts in a timely and effective manner on these incidents.

Our technical programs are also making great strides. The NIPC's work with private companies has been well received, in that SANS awarded us the 2000 Security Technology Leadership Award for members of our Special Technologies Applications Unit.

The NIPC is deepening its relationships between itself and other Federal agencies. For example, we have reached and finalized a formal agreement just this week with the Federal Aviation Administration. NIPC's Interagency Coordination Cell is fostering cooperation among investigative agencies. Several task forces have already begun based upon this work within this cell.

We are currently negotiating agreements with various other ISACs which will further improve the information-sharing process. As mentioned, our training program has trained over 4,000 Federal, State, local and foreign law enforcement personnel in computer and network investigations.

The NIPC is the sector lead for the emergency law enforcement services sector. On March 2, 2001, we delivered the sector plan to the White House. The ELES plan provides a toolbox to assist some 18,000 police and sheriffs departments in protecting their data and communications systems from attack.

It was the first plan to be completed and was very favorably received at the Partnership for Critical Infrastructure Security meeting and was given as a model for other sectors. Since the local police and sheriffs departments are usually among the first responders to an incident, the protection of their data and communications systems is vital to public safety and national security. In short, I think we have a robust program now.

As proud as I am of the NIPC's accomplishments, we must look to the future. I am focused on implementing a strategic planning effort that will produce measurable results as we face challenges ahead. Infrastructure protection is an issue that is bigger than one agency and any one private sector entity. We must develop meaningful partnerships between the public and private sectors, as well as internationally, to protection our Nation.

The NIPC will be striving to take an ever greater leadership role in this effort, and we will be doing this in close partnership with the Subcommittee's work in this area, as well as the administration's revisions to the national plan.

Again, I thank you.

[The prepared statement of Mr. Dick follows:]

STATEMENT OF RONALD L. DICK, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Madame Chairperson, Ranking Member Kyl, and members of the subcommittee, thank you for inviting me here today to testify about the recommendations outlined in the General Accounting Office (GAO) report titled "CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges in Developing National Capabilities." Holding this hearing once again demonstrates your personal commitment to improving the security of our critical infrastructures and this subcommittee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. One recent study observed "12,085 attacks on over 5,000 distinct Internet hosts belonging to more than 2,000 distinct organizations during a three-week period."[1] My testimony today will address what has been accomplished and what still needs to be done to implement the GAO report's recommendations. Our assessment of the overall report is contained in our testimony of May 22, 2001 before this subcommittee.

At the outset, let me say how pleased I am here today with GSA's Assistant Commissioner Sallie McDonald of FedCIRC and Deputy Special Agent in Charge of the Financial Crimes Division Jim Savage of the U.S. Secret Service. Assistant Commissioner McDonald's statement explains in detail the close working relationship that GSA's FedCIRC has with the NIPC, so I won't dwell on that here.

The GAO's recommendations fell into several broad categories, including: enhancing capacity for strategic analysis; monitoring field implementation of NIPC performance measures; completing the Emergency Law Enforcement Services Sector Plan; improving cooperative relationships between the NIPC and its federal part-

[1] David Moore, Geoffrey M. Voelker and Stefan Savage, "Inferring Internet Denial-of-Service Activity," May 2001.

ners; and furthering information sharing between the NIPC, the Information Sharing and Analysis Centers (ISACs) and the public.

Nevertheless, the Center has made great strides in achieving its mission under Presidential Decision Directive (PDD)63 over the past three years. In his prepared statement for the May 22, 2001 hearing, GAO's Director of Information Security, Mr. Robert F. Dacey, stated:

> First, the NIPC has provided valuable coordination and technical support to FBI field offices, which have established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC has supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for the NIPC field squads and teams.

Over the past three years, NIPC has provided training for almost 4,000 participants. The NIPC's training program complements training offered by the FBI's Training Division as well as training offered by the Department of Defense and the National Cybercrime Training Partnership. Trained investigators are essential to our successfully combating computer intrusions.

Enhancing Capacity for Strategic Analysis

The GAO report recommended that the NIPC develop a comprehensive, written plan for strategic analysis. While we have numerous documents reflecting strategic and tactical planning, I agree that more work needs to be done. As the GAO report noted, our progress in this area has been impeded by the personnel shortfalls and management discontinuities within the interagency Analysis and Warning Section. I am pleased to report progress in this area with the arrival in April of a Central Intelligence Agency (CIA) senior officer, detailed for a sustained period as the Section Chief, and the recent selection of an National Security Agency (NSA) officer as the Chief of the Analysis and Information Sharing Unit within that section.

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

As we work on these four strategic directions: attack prediction, prevention, detection, and mitigation, we will have many opportunities to stretch our capabilities. With respect to all of these, the NIPC is committed to continuous improvement through a sustained process of documenting "lessons learned" from significant cyber events. We have already begun one such lessons learned study in connection with the recent LEAVES worm event. The NIPC also remains committed to achieving all of its objectives while upholding the fundamental rights of our citizenry, including the fundamental right to privacy.

The NIPC is excited by each of these strategic directions. I will lead a senior planning offsite later this summer and I expect to have the documented strategic plan completed by December. We are conducting this planning in a climate of intensified cyber attacks in by a growing number of automated tools that make effective hacking literally child's play. For instance, hackers are preying on the growing number

of American home computer users for whom computers and cable modems are merely appliances rather than hobbies. These millions of home computers often lack the latest security updates, intrusion detection capabilities, and anti-virus signatures.

The GAO also recommended that the NIPC ensure that its Special Technologies and Applications Unit have the computer and communications resources necessary to analyze investigative data. The NIPC has already begun to address this issue by through the continued implementation of the NIPC's "data warehousing and data mining" project. This will allow the NIPC to retrieve incident data originating from multiple sources. Data warehousing includes the ability to conduct real-time allsource analysis and report generation. This initiative is ongoing and will require multiple year funding to reach maximum potential.

Monitoring Implementation of Field Perforrnance Measures

The GAO recommended that the NIPC monitor implementation of new performance measures to ensure that they result in FBI Field Offices fully reporting information on computer crime complaints to the NIPC. The NIPC continues to monitor the open investigations of all the field offices and field performance in monthly statistical reports. Along with this, the FBI field offices report information on potential computer crimes by documenting and uploading reports of these incidents to the FBI's automated case support system. These records are searchable and available to NIPC Headquarters personnel who correlate the incidents with other pending investigations. The placement of the NIPC at the FBI endows the Center with both the authorities and the ability to combine law enforcement information flowing into the NIPC from the FBI Field Offices with other information streams derived from open, confidential, and classified sources. This capability is unique in the federal government. The NIPC views monitoring field office reporting as an ongoing action.

Completion of the Emergency Law Enforcement Services Plan

This task is completed. The NIPC serves as sector liaison for Emergency Law Enforcement Services (ELES) sector at the request of the FBI. The NIPC completed the ELES Sector Plan in February, 2001. The ELES Sector Plan was the first completed sector report under PDD–63 and was delivered to the White House on March 2, 2001. At the Partnership for Critical Infrastructure Security in Washington, D.C., in March, 2001, the ELES Plan was held up as a model for the other sectors. The NIPC also sponsored the formation of the Emergency Law Enforcement Services Sector forum, which meets quarterly to discuss issues relevant to sector security planning. The Forum contains federal, state, and local representatives. The next meeting of the forum is scheduled for September, 2001.

The Plan was the result of two years' work in which the NIPC surveyed law enforcement agencies concerning the vulnerabilities of their infrastructure. Following the receipt of the survey results, the NIPC and the ELES Forum produced the ELES Sector Plan. The NIPC also produced a companion "Guide for State and Local Law Enforcement Agencies" that provides guidance and a "toolkit" that law enforcement agencies can use when implementing the activities suggested in the Plan.

The importance of the ELES Sector Plan and the Guide cannot be overstated. These documents will aid some 18,000 police departments located in towns and neighborhoods to better protect themselves from attack. Since the local police are usually among the first responders to any incident threatening public safety, their protection is vital to our national security.

Enhancing Cooperative Relationships Among Federal Agencies

The GAO recommended that the NIPC formalize relationships between itself, other federal entities, and private sector ISACs, so a clear understanding of what is expected from the respective organizations exists. The NIPC has established effective information sharing and cooperative investigative relationships across the U.S. Government. A formal Memoranda of Agreement was just completed with the Department of Transportation's Federal Aviation Administration (FAA) which will govern how information is shared between FAA and NIPC and how that information will be communicated. This MOA formalizes a long-standing informal process of information sharing between NIPC and FAA. Informal arrangements have already been established with the Federal Communications Commission, Department of Transportation's (DOT) National Response Center, DOT Office of Pipeline Safety, Department of Energy's Office of Emergency Management, and others, which allow the NIPC to receive detailed sector-specific incident reports in a timely manner. Formal MOAs should soon be completed with several other agencies, including the Na-

tional Coordinating Center for Telecommunications and the Federal Emergency Management Agency's National Fire Administration.

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

The NIPC functions in a task force like way, coordinating investigations in a multitude of jurisdictions, both domestically and internationally. This is essential due to the transnational nature of cyber intrusions. As NIPC coordinates a myriad of investigative efforts within the FBI, it is not unlike the way the air traffic control system manages the stream of aircraft traffic across the United States and around the world.

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

Senior leadership positions in the NIPC are held by personnel from several agencies. The position of NIPC Director is reserved for a senior FBI executive. The Deputy Director of the NIPC is a two-star Navy Rear Admiral and the Executive Director is detailed from the Air Force Office of Special Investigations. The Section and Unit Chiefs in the Computer Investigation and Operations Section and the Training, Outreach, and Strategy Section are from the FBI. The Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service. The Section Chief of the Analysis and Warning Section is from the CIA and his deputy is a senior FBI agent. The head of the NIPC Watch and Warning Unit is reserved for a uniformed service officer, and the head of the Analysis and Information Sharing Unit is reserved for a National Security Agency manager.

While the Center has representatives from several U.S. Government agencies, staffing continues to be a challenge. Non-FBI personnel are provided to the Center on a non-reimbursable basis. Agencies have responded to the NIPC's requests for detailees by saying that they are constrained from sending personnel due to lack of funds. It is vitally important that agencies be provided with sufficient funds for the assignment of detailees to the NIPC to support its strategic analysis mission.

As part of its emphasis on cooperation, the GAO recommended that the NIPC ensure that its Key Asset Initiative is integrated with the DoD and Critical Infrastructure Assurance Office (CIAO) programs. The objective of the Key Asset Initiative is to develop and maintain a database of information concerning "key assets" within each FBI Field Office's jurisdiction as part of a broader effort to protect the critical infrastructures against both physical and cyber threats. This initiative benefits national security planning efforts by providing a better understanding of the location, importance, and contact information for critical infrastructure assets across the United States. The NIPC has worked with the DoD and the CIAO on its Key Asset Initiative by involving them in the training of agents that work on the Initiative and by meeting with them regarding their programs. The NIPC and the Department of Defense are working toward a Memorandum of Understanding that will assist in defining cooperative efforts.

The NIPC has taken other initiatives as well in fulfilling its role to lead the critical infrastructure protection effort. This is evidenced by its coordinating actions as Chair of the Incident Response SubGroup of the Information Infrastructure Protection and Assurance Group established by NSPD–1. The NIPC also routinely disseminates information through its participation in task forces and working;" groups that meet regularly. NIPC senior leadership participates in weekly senior level meetings to exchange strategic level information with the Assistant Secretary of De-

fense for Command, Control, Communication and Intelligence. Further collaboration is demonstrated through the NIPC's designation as chair of one of the subcommittees that is drafting version two of the National Plan.

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

The NIPC sends out advisories on an ad hoc basis which are infrastructure warnings to address cyber or infrastructure events with possible significant impact. These are distributed to partners in private and public sectors. A number of recent advisories sent out by the NIPC (see for example Advisory 01–014, titled "New Scanning Activity (with W32–LEAVES.worm) Exploiting SubSeven Victims ") serve to demonstrate the continued collaboration between the NIPC and its partner FedCIRC. The NIPC serves as a member of FedCIRC's Senior Advisory Council and has daily contact with that entity as well as a number of others including NSA and DoD's Joint Task Force Computer Network Operations (JTF–CNO). On issues of national concern, the recent incident involving the LEAVES and IDA CODE RED Worms are good examples of the NIPC's success in working with the National Security Council and our partner agencies to disseminate information and coordinate strategic efforts in a timely and effective manner.

In addition to its public web-based warning messages, the NIPC sends out tailored products to the federal government, the Information Sharing and Analysis Centers (ISACs), and InfraGard partners. Depending on the audience, these products may be classified or unclassified. The Monthly Highlights are sent out to policy/decision makers, and Cybernotes (which lists current exploited software vulnerabilities and other malicious code) is sent to system and network administrators. The NIPC Daily Report contains timely items of interest and significant cyber/infrastructure activity relevant to the infrastructure protection community and is sent to some of our federal partners as well as secure InfraGard members.

In response to PDD–63 provisions that all executive departments and agencies shall share with the NIPC information about threats and attacks on their systems, the NIPC–FAA MOU can serve as a forerunner for agreements to promote information sharing with the other 70 plus executive branch agencies. The NIPC has developed a model agreement can be modified to suit individual agency requirements. The execution of these agreements will confirm the obligations and clarify information sharing and warning procedures between the federal agencies and the NIPC. These model agreements will be communicated to federal executive branch agencies to open a dialogue on formalizing their relationship with the NIPC. These agreements will also address the GAO's recommendation that relationships between the NIPC and other federal entities be formalized so that a clear understanding of what is expected from the respective organizations exists. The NIPC anticipates that this will be an ongoing effort to create, monitor, and maintain these information sharing relationships.

Improving Information Sharing

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

As noted in the GAO report, over the past two years the NIPC and the North American Electric Reliability Council (NERC)-the ISAC for the electric power sectorhave established an indications, analysis and warning program (IAW) program, which makes possible the timely exchange of information valued by both the NIPC and the electric power sector. This relationship is possible because of a commitment both on the part of NERC and the NIPC to build cooperative relations. The close NERC–NIPC relationship is no accident but the result of two interrelated sets

of actions. First, as Eugene Gorzelnik, Director of Communications for the NERC, stated in his prepared statement at the May 22, 2001 hearing:

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

Second, the NIPC and NERC worked for over two years on building the successful partnership that now exists. It did not just happen. It took dedicated individuals in both organizations to make it happen. It is this success and dedication to achieving results that the NIPC is working to emulate with the other ISACs.

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

ISACs have been established for the critical infrastructure sectors of banking and finance, information and telecommunications, electric power, and emergency law enforcement services. They have not yet been established for the remaining sectors enumerated in PDD–63. A model NIPC–ISAC agreement has been prepared to promote the sharing of information with these existing ISACs and ISACs yet to be formed. Agreements are being negotiated between the NIPC and the Telecommunications ISAC, as well as the NIPC and the United States Fire Administration (emergency fire services ISAC). The execution of these agreements should pave the way for NIPC agreements with other ISACs. The NIPC welcomes the participation of the sector lead agencies and the sector coordinators to improving the information sharing process with the ISACs. These efforts are ongoing.

The NIPC also shares information via its InfraGard Initiative. All 56 FBI field offices now have InfraGard chapters. Just in the last six months the InfraGard Initiative has added over 1000 new members to increase the overall membership to over 1600. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service we provide to InfraGard members free of charge. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices and several of its Resident Agencies (subdivisions of the larger field offices).

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

InfraGard held its first national congress from June 12–14, 2001. This conclave provided an excellent forum for NIPC senior managers and InfraGard members to exchange ideas. InfraGard's success is directly related to private industry's involvement in protecting its critical systems, since private industry owns almost all of the infrastructures. The dedicated work of the NIPC and the InfraGard members is paying off. InfraGard has already prevented cyber attacks by discretely alerting

InfraGard members to compromises on their systems. On May 3, 2001, the InfraGard initiative received the 2001 WorldSafe Internet Safety Award from the Safe America Foundation for its efforts.

CONCLUSION:

I remain encouraged by the progress the NIPC has made in its first three years. Our multiagency partnership has developed unique national capabilities that have never before been achieved. We will continually improve in the coming years in order to master the perpetually evolving challenges involved with infrastructure protection and information assurance. The GAO recommendations are all being addressed and I plan to keep the subcommittee updated on our progress. Thank you for inviting me here today and I welcome any questions you have.

Chairperson FEINSTEIN. Thanks very much, Mr. Dick. Thank you for keeping within the time limit. I appreciate it.

We will go to Mr. Dacey, of the GAO, who did the report.

Mr. Dacey?

STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, GENERAL ACCOUNTING OFFICE, WASHINGTON, D.C.

Mr. DACEY. Madam Chairwoman and Senator Kyl, I am pleased to be here today to discuss our review of the National Infrastructure Protection Center and its progress in developing the capabilities outlined in Presidential Decision Directive 63. As you requested, I will briefly summarize my written statement. Our testimony highlights key findings in our report on the NIPC which you released in May of this year.

PDD–63, issued in May 1998, outlined our Government's strategy to protection our Nation's critical infrastructures from hostile attacks, especially computer-based attacks, and specifically assigned the NIPC, within the FBI, responsibility for providing comprehensive analysis and issuing timely warnings on threats, vulnerabilities, and attacks, facilitating and coordinating our Government's response to cyber incidents, and promoting outreach and information-sharing.

While NIPC efforts have laid a foundation for developing these capabilities, significant challenges remained at the close of our review. For example, the NIPC has issued numerous analyses to support investigations of individual incidents, but has developed only limited capabilities for broader strategic analysis of threat and vulnerability data.

Three factors have contributed to these limitations. First, there is no generally accepted methodology for strategic analysis of cyber-based threats. According to officials in the intelligence and national security communities, developing such a methodology would require an intense interagency effort and dedication of resources.

Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because Federal agencies have not provided the originally anticipated number of detailees.

Third, the NIPC did not have industry-specific data on critical infrastructures, which under PDD–63 were to be provided for each of the industry sectors by industry representatives and the designated Federal lead agencies.

The NIPC has established a rudimentary capability to identify attack that appear imminent and alert Government and the pri-

vate sector. However, the NIPC's ability to issue warnings promptly has been impeded by several factors: first, the lack of a comprehensive national framework for promptly obtaining and analyzing information indicating that attack may be imminent or underway; two, a shortage of skilled staff; three, the need to ensure that NIPC does not raise undue alarm for insignificant incidents; and, four, the need to ensure that sensitive information is protected.

However, I want to emphasize a more fundamental impediment. Specifically, the entities involved in the Government critical infrastructure protection efforts did not share a common interpretation of NIPC's roles and responsibilities. Further, the relationships between the NIPC, the FBI, and the National Coordinator for Security Infrastructure Protection and Counterterrorism are unclear regarding who has direct authority for setting NIPC priorities and procedures and providing NIPC oversight.

The NIPC has had greater success in providing technical support and coordination with the NIPC squads and teams in the various FBI field offices. In addition, the NIPC has developed and implemented procedures for establishing crisis action teams to respond to potentially serious computer-based incidents.

In the area of establishing information-sharing partnerships, progress has varied. NIPC's InfraGard program for sharing information on computer-based threats and incidents with private sector companies has steadily gained enrollment, as we have previously discussed here. Also, the NIPC has provided training to Government entities and has advised foreign governments that are establishing centers similar to the NIPC.

However, at the close of our review in February, a two-way information-sharing partnership with the NIPC had been established with only one of the four industry information-sharing and analysis centers that had been established at that time. Similarly, the NIPC and FBI had made only limited progress in developing a data base of the most important components of the Nation's critical infrastructures, referred to as the Key Asset Initiative. In addition, the NIPC and other Government entities, such as the Department of Defense and the Secret Service, had not developed fully productive information-sharing and cooperative relationships.

The NIPC is aware of the challenges it faces and has taken some steps to address them. In addition, the administration is reviewing its critical infrastructure protection strategy, including the way that the Federal Government is organized to manage this effort. Our report includes a variety of recommendations that are pertinent to these efforts.

Madam Chairwoman and Senator Kyl, this concludes my statement. Thank you.

Chairperson FEINSTEIN. Since you didn't use up all your 5 minutes, could you just speak on your recommendations, specifically two of them, that the Attorney General direct the FBI Director to direct the NIPC Director to ensure to develop a comprehensive written plan for establishing analysis and warning capabilities as well as to do several other things. These recommendations are at the bottom of page 15 of the Executive Summary and the top of page 14—quickly, what progress has been made?

Mr. DACEY. Madam Chairwoman, we did not do any follow-up work beyond the work that we had done in terms of February, but at that point in time the recommendations really kind of paralleled the kind of issues that we saw in February. I don't know if Mr. Dick would care to elaborate on the actions more fully to address those specific recommendations.

Chairperson FEINSTEIN. Fine. I will ask him, then, at a later time.

[The prepared statement of Mr. Dacey follows:]

STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to discuss our review of the National Infrastructure Protection Center (NIPC). As you know, the NIPC is an important element of our government's strategy to protect our national infrastructures from hostile attacks, especially computer-based attacks. This strategy was outlined in Presidential Decision Directive (PDD) 63, which was issued in May 1998.

My statement summarizes the key findings in our report on the NIPC, which you released in May.[1] That report is the result of an evaluation we performed at the request of you, Madam Chairwoman; Senator Kyl; and Senator Grassley. As you requested, the report describes the NIPC's progress in developing national capabilities for analyzing cyber threats and vulnerability data and issuing warnings, enhancing its capabilities for responding to cyber attacks, and establishing information-sharing relationships with government and private-sector entities.

Overall, we found that progress in developing the analysis, warning, and informationsharing capabilities called for in PDD 63 has been mixed. The NIPC has initiated a variety of critical infrastructure protection efforts that have laid a foundation for future governmentwide efforts. In addition, it has provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review in February 2001, the analytical and information-sharing capabilities that PDD 63 asserts are needed to protect the nation's critical infrastructures had not yet been achieved, and the NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort. An underlying contributor to the slow progress is that the NIPC's roles and responsibilities had not been fully defined and were not consistently interpreted by other entities involved in the government's broader critical infrastructure protection strategy. Further, these entities had not provided the information and support, including detailees, to the NIPC that was envisioned by PDD 63.

The NIPC is aware of the challenges it faces and has taken some steps to address them. In addition, the administration is reviewing the federal critical infrastructure protection strategy, including the way the federal government is organized to manage this effort. Our report includes a variety of recommendations that are pertinent to these efforts, including addressing the need to more fully define the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with private-sector and federal entities.

The remainder of my statement will describe the NIPC's role in the government's broader critical infrastructure protection efforts, as outlined in PDD 63, and its progress, as of the close of our review, in three broad areas: developing analysis and warning capabilities, developing response capabilities, and establishing information-sharing relationships.

BACKGROUND

Since the early 1990s, the explosion in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the wayorganizations conduct business, making communications faster and access to data easier. However, this widespread interconnectivity has increased the risks to computer systems and, more importantly, to the critical operations and infrastructures that these systems support, such as telecommunications, power distribution, national defense, and essential government services.

[1] Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities (GAO–O1–323, April 25, 2001).

Malicious attacks, in particular, are a growing concern. The National Security Agency has determined that foreign governments already have or are developing computer attack capabilities, and that potential adversaries are developing a body of knowledge about U.S. systems and methods to attack them. In addition, reported incidents have increased dramatically in recent years. Accordingly, there is a growing risk that terrorists or hostile foreign states could severely damage or disrupt national defense or vital public operations through computer-based attacks on the nation's critical infrastructures. Since 1997, in reports to the Congress, we have designated information security a governmentwide high-risk area. Our most recent report in this regard, issued in January,[2] noted that, while efforts to address the problem have gained momentum, federal assets and operations continue to be highly vulnerable to computer-based attacks.

To develop a strategy to reduce such risks, in 1996, the President established a Commission on Critical Infrastructure Protection. In October 1997, the commission issued its report,[3] stating that a comprehensive effort was needed, including "a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats." The report said that the Federal Bureau of Investigation (FBI) had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In May 1998, PDD 63 was issued in response to the commission's report. The directive called for a range of actions intended to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious computer-based attacks. The directive established a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism under the Assistant to the President for National Security Affairs. Further, the directive designated lead agencies to work with private-sector entities in each of eight industry sectors and five special functions. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electric power industry.

PDD 63 also authorized the FBI to expand its NIPC, which had been originally established in February 1998. The directive specifically assigned the NIPC, within the FBI, responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to cyber incidents; providing law enforcement investigation and response; monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing.

MULTIPLE FACTORS HAVE LIMITED DEVELOPMENT OF ANALYSIS AND WARNING CAPABILITIES

PDD 63 assigns the NIPC responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities as well as timely warnings of potential and actual attacks. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent.

Since its establishment in 1998, the NIPC has issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. These analyses have included (1) situation reports related to law enforcement investigations, including denial-of-service attacks that affected numerous Internet-based entities, such as eBay and Yahoo and (2) analytical support of a counterintelligence investigation. In addition, the NIPC has issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

Strategic analysis to determine the potential broader implications of individual incidents has been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing

---

[2] High-Risk Series: Information Management and Technology (GAO/HR–97–9, February 1, 1997); High-Risk Series: An Update (GAO/HR–99–1, January, 1999); High-Risks Series: An Update (GAO–01–263, January 2001).

[3] Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection, October 1997.

risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

Three factors have hindered the NIPC's ability to develop strategic analytical capabilities.

• First, there is no generally accepted methodology for analyzing strategic cyberbased threats. For example, there is no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.

• Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because other federal agencies have not provided the originally anticipated number of detailees. For example, as of the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of the NIPC's 3-year existence. In addition, the NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.

• Third, the NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work in February, only three industry assessments had been partially completed, and none had been provided to the NIPC.

To provide a warning capability, the NIPC established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. As of February, the unit had issued 81 warnings and related products since 1998, many of which were posted on the NIPC's Internet web site. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. The NIPC's ability to issue warnings promptly is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

However, I want to emphasize a more fundamental impediment. Specifically, evaluating the NIPC's progress in developing analysis and warning capabilities is difficult because the federal government's strategy and related plans for protecting the nations critical infrastructures from computer-based attacks, including the NIPC's role, are still evolving. The entities involved in the government's critical infrastructure protection efforts have not shared a common interpretation of the NIPC's roles and responsibilities. Further, the relationships between the NIPC, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council have been unclear regarding who has direct authority for setting NIPC priorities and procedures and providing NIPC oversight. In addition, the NIPC's own plans for further developing its analytical and warning capabilities were fragmented and incomplete. As a result, there were no specific priorities, milestones, or program performance measures to guide NIPC actions or provide a basis for evaluating its progress.

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in PDD 63, including provisions related to developing analytical and warning capabilities that are currently assigned to the NIPC. On May 9, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and reviewing how the government is organized to deal with information security issues.

In our report, we recommend that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

• establish a capability for strategic analysis of computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;

• require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and

• clearly define the role of the NIPC in relation to other government and private-sector entities.

NIPC COORDINATION AND TECHNICAL SUPPORT HAVE BENEFITED INVESTIGATIVE AND RESPONSE CAPABILITIES

PDD 63 directed the NIPC to provide the principal means of facilitating and coordinating the federal government's response to computer-based incidents. In response the NIPC undertook efforts in two major areas: providing coordination and technical support to FBI investigations and establishing crisis management capabilities.

First, the NIPC provided valuable coordination and technical support to FBI field offices, which established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for the NIPC field squads and teams.

While these efforts benefited investigative efforts, FBI and NIPC officials told us that increased computer capacity and data transmission capabilities would improve their ability to promptly analyze the extremely large amounts of data that are associated with some cases. In addition, FBI field offices were not yet providing the NIPC with the comprehensive information that NIPC officials say is needed to facilitate prompt identification and response to cyber incidents. According to field office officials, some information on unusual or suspicious computerbased activity had not been reported because it did not merit opening a case and was deemed to be insignificant. To address this problem, the NIPC established new performance measures related to reporting.

Second, the NIPC developed crisis management capabilities to support a multiagency response to the most serious incidents from the FBI's Washington, D.C., Strategic Information Operations Center. From 1998 through early 2001, seven crisis action teams had been activated to address potentially serious incidents and events, such as the Melissa virus in 1999 and the days surrounding the transition to the year 2000, and related procedures have been formalized. In addition, the NIPC coordinated development of an emergency law enforcement plan to guide the response of federal, state, and local entities.

To help ensure an adequate response to the growing number of computer crimes, we recommend in our report that the Attorney General, the FBI Director, and the NIPC Director take steps to (1) ensure that the NIPC has access to needed computer and communications resources and (2) monitor implementation of new performance measures to ensure that field offices fully report information on potential computer crimes to the NIPC.

PROGRESS IN ESTABLISHING INFORMATION-SHARING RELATIONSHIPS HAS BEEN MIXED

Information sharing and coordination among private-sector and government organizations are essential for thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as we testified in July 2000[4] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

NIPC success in this area has been mixed. For example, the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, had grown to about 500 member organizations as of January 2001 and was viewed by the NIPC as an important element in building trust relationships with the private sector. NIPC officials recently told us that InfraGard membership has continued to increase. However, of the four information sharing and analysis centers that had been established as focal points for infrastructure sectors, a two-way, informationsharing partnership with the NIPC had developed with only one-the electric power industry. The NIPC's dealings with two of the other three centers primarily consisted of providing information to the centers without receiving any in return, and no procedures had been developed for more interactive information sharing. The NIPC's information-sharing relationship with the fourth

[4] Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation (GAO/T–AIMD–00–268, July 26, 2000). Testimony before the subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives.

center was not covered by our review because the center was not established until mid-January 2001, shortly before the close of our work.

Similarly, the NIPC and the FBI have made only limited progress in developing a database of the most important components of the nation's critical infrastructures—an effort referred to as the Key Asset Initiative. While FBI field offices had identified over 5,000 key assets, at the time of our review, the entities that own or control the assets generally had not been involved in identifying them. As a result, the key assets recorded may not be the ones that infrastructure owners consider to be the most important. Further, the Key Asset Initiative was not being coordinated with other similar federal efforts at the Departments of Defense and Commerce.

In addition, the NIPC and other government entities had not developed fully productive information-sharing and cooperative relationships. For example, federal agencies have not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's Federal Computer Incident Response Capability. Further, NIPC and Defense officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts.

The NIPC has been more successful in providing training on investigating computer crime to government entities, which is an effort that it considers an important component of its outreach efforts. From 1998 through 2000, the NIPC trained about 300 individuals from federal, state, local, and international entities other than the FBI. In addition, the NIPC has advised several foreign governments that are establishing centers similar to the NIPC.

To improve information sharing, we recommend in our report that the Assistant to the President for National Security Affairs

- direct federal agencies and encourage the private sector to better define the types of information necessary and appropriate to exchange in order to combat computer-based attacks and to develop procedures for performing such exchanges,
- initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, and
- resolve discrepancies in requirements regarding computer incident reporting by federal agencies.

In our report, we also recommend that the Attorney General task the FBI Director to

- formalize information-sharing relationships between the NIPC and other federal entities and industry sectors and
- ensure that the Key Asset Initiative is integrated with other similar federal activities.

In conclusion, it is important that the government ensure that our nation has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damage to our critical infrastructures. The analysis, warning, response, and information-sharing responsibilities that PDD 63 assigned to the NIPC are important elements of this capability. However, as our report shows, developing the needed capabilities will require overcoming many challenges. Meeting these challenges will not be easy and will require clear central direction and dedication of expertise and resources from multiple federal agencies, as well as private sector support.

Madame Chairwoman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

CONTACT AND ACKNOWLEDGMENTS

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

Chairperson FEINSTEIN. Ms. McDonald, welcome.

STATEMENT OF SALLIE McDONALD, ASSISTANT COMMISSIONER, OFFICE OF INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION, GENERAL SERVICES ADMINISTRATION, WASHINGTON, D.C.

Ms. MCDONALD. Thank you. Good afternoon, Madam Chairwoman and Ranking Member Kyl. I wish to thank you for the opportunity to offer testimony with regard to the National Infrastructure Protection Center.

The Federal Computer Incident Response Center, or FedCIRC, is a component of GSA's Federal Technology Service. It is the central coordination entity for dealing with computer security-related incidents affecting computer systems within the Federal civilian agencies of the U.S. Government.

FedCIRC and NIPC are both crucial to effective cyber defense, but serve differing roles to the Federal community. FedCIRC's role is to provide incident response and handling reports from agencies. When an agency reports an incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident.

The NIPC, on the other hand, collects incident reports and is responsible for providing threat assessments, vulnerability studies, warnings——

Chairperson FEINSTEIN. Ms. McDonald, I am going to interrupt you because we have 4 minutes left in this vote.

Ms. MCDONALD. OK.

Chairperson FEINSTEIN. I hope people will wait. We will come back right away, if you don't mind, and excuse us for a couple of minutes.

[The Subcommittee stood in recess from 2:33 p.m. to 2:50 p.m.]

Chairperson FEINSTEIN. We will resume.

Ms. McDonald, again, we are sorry to interrupt your testimony, but please continue. We may interrupt you once again because Senator Cleland is coming and wanted to introduce one of the witnesses on the next panel and he is limited in time, so we might interrupt you once again.

Ms. MCDONALD. No problem.

Chairperson FEINSTEIN. Thank you.

Ms. MCDONALD. As I was saying, the NIPC's responsibility is to collect incident reports and provide threat assessments, vulnerability studies, warnings, and coordinate the Federal Government's investigative response to attacks.

Upon receiving an incident report from a Federal agency, FedCIRC evaluates and categorizes the incident with respect to its impact and severity. If criminal activity is indicated, FedCIRC informs the reporting agency of the requirement to immediately contact their inspector general or the NIPC. Should the incident appear to have originated from a foreign country, FedCIRC categorizes it as having potential national security implications and immediately contacts both the National Security Agency and the NIPC. The reporting agency is subsequently notified of such action by FedCIRC.

There is an ongoing discussion between the NIPC and FedCIRC to improve information-sharing and analytical efforts, and to edu-

cate agencies of the value of rapid involvement of the NIPC when incidents occur. Effective incident analysis is the product of multiple-source data collection efforts, collaboration to quantify related information, and determination of the potential for proliferation and damage.

Over the past few years, a virtual network of partners has evolved. This virtual network includes FedCIRC, the NIPC, the National Security Agency, the Department of Defense, industry, academia, and individual incident response components within Federal agencies.

Though their missions vary in scope and responsibility, this virtual network enables the Federal Government to capitalize on the individual technical strengths, each organization's strategic positioning within the national infrastructure, and their access to a variety of information resources.

Bridging the disparate boundaries has been a formidable challenge, and although there is still work to be done in this area, the commitment of the leadership in each organization is on the right path to build the framework for the fluid and cooperative exchange of information.

Critical infrastructure protection efforts, and more specifically those for cyber defense, are a relatively new requirement in Government and in the private sector. Only recently have these efforts been singled out as a priority for Federal agencies.

As Government direction for reporting the occurrence of incidents has been promulgated, attempts by agencies to develop related policies and procedures has sometimes been divergent because of differing individual interpretations and misunderstanding. FedCIRC and the NIPC are working diligently to jointly assess problem areas, more clearly define agency responsibilities for reporting incidents, and working with agencies to ensure that they have the proper processes and procedures in place to respond to and prevent attacks on their information systems.

Madam Chairperson, the information presented today highlights the high degree of cooperation that exists among Government agencies and the critical and effective relationship that exists between FedCIRC and the NIPC. Though all contribute individually to critical infrastructure protection, our strength in protecting information systems governmentwide lies in collaboration and coordination efforts. I trust that you will derive from my remarks an understanding of the cyber threat and response issues, and also an appreciation of the joint commitment to infrastructure protection of the FedCIRC and the NIPC.

Thank you very much.

[The prepared statement of Ms. McDonald follows:]

STATEMENT OF SALLIE MCDONALD, ASSISTANT COMMISSIONER, OFFICE OF INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION

Good afternoon Madam Chairwoman and members of the Subcommittee. I am Sallie McDonald, the Assistant Commissioner for the GSA, FTS, Office of Information Assurance and Critical Infrastructure Protection. I wish to thank you for the opportunity to offer testimony with regard to the National Infrastructure Protection Center (NIPC).

The Federal Computer Incident Response Center or FedCIRC, is a component of GSA's Federal Technology Service. As designated by the Government Information Security Reform Act, it is the central coordination entity for dealing with computer

security related incidents affecting computer systems within the Federal civilian agencies and Departments of the United States Government.

FedCIRC was established as a pilot by NIST in 1996 under the Office of Management and Budget (OMB) policy authority as the primary means for civilian Federal agencies to share information on externally generated security incidents and common vulnerabilities. This was recognized as an important activity given the shared risk environment that results from a rise in interconnected systems across government and with connection to the Internet which increases public access. FedCIRC became operational in 1998 and was transferred to GSA. FedCIRC's role was then and is today, one of assisting agencies and sharing information under the overall security policy framework established by OMB. FedCIRC is not intended to substitute for adequate agency security practices or compete with the role of law enforcement or national security authorities in addressing more serious types of attacks.

GSA reports at least quarterly to OMB on matters such as the number and nature of security incidents reported by the agencies, whether the incidents are the result of exploits of vulnerabilities for which known repairs are readily available, and whether FedCIRC has any specific recommendations for changes to OMB security policy or the National Institute of Standards and Technology (KIST) security guidance.

By definition, a "computer security incident" encompasses any violation of an established or implied security policy or statute. Incidents include but are not necessarily limited to activities such as attempts to gain unauthorized access to government systems or data, disruption of service, unauthorized use of computing resources and changes to system hardware or software without consent of the owner.

FedCIRC and the NIPC are both crucial to effective cyber defense but serve differing roles to the Federal community. FedCIRC's role is to provide incident response and handling support to agencies. When an agency reports an incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident. The NIPC, on the other hand, collects incident reports and is responsible for providing threat assessments, vulnerability studies, warnings, and the coordination of the Federal government's investigative response to attacks.

Upon receiving an incident report from a Federal agency, FedCIRC evaluates and categorizes the incident with respect to its impact and severity. If criminal activity is indicated, FedCIRC informs the reporting agency of the requirement to immediately contact their Inspector General or the NIPC. Should the incident appear to have originated from a foreign country, FedCIRC categorizes it as having potential national security implications and immediately contacts both the NSIRC and the NIPC. The reporting agency is subsequently notified of such action by FedCIRC. There is ongoing discussion between the NIPC and FedCIRC to improve information sharing and analytic efforts and to educate agencies of the value of rapid involvement of the NIPC when incidents occur. When the escalation of an incident has the potential for widespread proliferation or damage, FedCIRC and the NIPC routinely pool their information and skills. FedCIRC is frequently requested by the NIPC to collaborate with multiple sources and the affected agency or agencies to gather more detailed information specific to a given incident. Cyber-incidents involving a pending or potential investigation are jointly handled in a manner that preserves sensitive cyber-evidence without adverse impact to the affected agency's mission functions or violation of constitutional law and applicable privacy statutes.

Effective incident analysis is a product of multiple source data collection efforts, collaboration to quantify related information, and determination of the potential for proliferation and damage. Over the past few years, a virtual network of partners has evolved. This virtual network includes FedCIRC, the NIPC, the National Security Agency's (NSA) National Security Incident Response Center (NSIRC), the Department of Defense's (DOD) Joint Taskforce for Computer Network Operations (JTF–CNO), industry, academia, and individual incident response components within Federal agencies. Though their missions vary in scope and responsibility, this virtual network enables the Federal government to capitalize on the individual technical strengths, each organization's strategic positioning within the national infrastructure and their access to a variety of information resources. Bridging the disparate boundaries has been a formidable challenge and although there is still work to be done in this area the commitment of the leadership in each organization is on the right path to build the framework for the fluid and cooperative exchange of information. The NIPC, NSIRC, JTF–CNO and FedCIRC are involved in a constant sharing of sensitive cyber-threat and incident data, correlating it with counter-terrorism and intelligence reports to develop strategic defenses, threat predictions and timely alerts. These efforts depend, not on any one participant, but on the unique

and valuable contributions of each organization. The NIPC, because of its relationships with industry, is able to solicit additional participation when the government deals with complex analysis issues. This broader spectrum brings together some of the nation's best talent to work on known and developing threats to the cyber infrastructure.

An excellent example of this collaboration is the Government's response to a very recent threat to the cyber infrastructure, know as the "Leaves Worm". This exercise clearly demonstrated how these collaborative relationships work and how each participant's contributions assist in assessing the damage potential. In June, the SANS Institute, a private sector organization, informed the NIPC of suspicious activities taking place in a large number of systems across the Internet. Widespread scanning was taking place to identify systems previously compromised by a relatively old trojan called "SubSeven." Since SubSeven is for all intents and purposes a remote control program, once identified, the perpetrator could gain full control of the infected system. It was through the SubSeven trojan that the Leaves Worm was being deposited on large numbers of systems around the globe but it was being accomplished without direct intervention by the perpetrator. Clearly we had a new worm of unknown potential and a new delivery method not previously seen. The hacker community, typically vocal in Internet chat rooms about new attacks or malicious code, showed no evidence of any knowledge of the Leaves Worm. The NIPC, DOJ, NSA, FedCIRC, CIA, Department of State, DoD, NCS, NSC, academia, industry software vendors, anti-virus engineers and security professionals quickly activated a collaborative communication network to share details as they analyzed captured code from publicly available web sites that were being used to propagate the worm. It was primarily due to the NIPC's relationship with industry that the volumes of information collected could be rapidly decoded, analyzed and reverse engineered to provide the anti-virus vendors with critical information to develop detection methods for their respective products. This episode serves as an excellent example of the progress various government and private organizations have made in coming together to work toward the common goal of protecting the nation's critical infrastructure.

The NIPC's responsibilities and relationships with various elements in the private sector, its activities as a member of the intelligence community and its lead role for counterterrorism contribute significantly to the FedCIRC's analytical ability by providing global threat information. Of significant value is the NIPC's ability to reach beyond governmental boundaries and draw on technical skills and information available from components in industry then share those resources with other members of the incident response community. The NIPC staff regularly communicates information to FedCIRC, which in many cases, provides deeper insight into developing situations and often can make the difference between thwarting an attack or tolerating the ensuing damage. Knowing the extent or pattern of incidents as they may impact the private sector, for example, may influence the development of an alert or advisory notice issued to government agencies.

Critical Infrastructure Protection efforts and, more specifically, those for cyber-defense are a relatively new requirement in government and in the private sector. Only recently have these efforts been singled out as a priority for Federal agencies. As government direction for reporting the occurrence of incidents has been promulgated, attempts by agencies to develop related policies and procedures have sometimes been divergent because of differing individual interpretation and misunderstanding. FedCIRC and the NIPC are working diligently to jointly assess problem areas, more clearly define agency responsibilities for reporting incidents, and working with agencies to ensure they have the proper processes and procedures in place to respond to and prevent attacks on their information systems.

The NIPC and FedCIRC routinely exchange information. This exchange is built upon a trust relationship and formalized with the detailing of FedCIRC staff personnel to the NIPC's Watch and Warning Unit. In addition alerts and advisories are frequently generated by the NIPC, NSIRC, or FedCIRC as a collaborative effort and represent a consensus when distributed to our constituents.

As a further example, to simplify the incident reporting process, the NIPC, NSA and FedCIRC have begun efforts to create a single uniform report process that will be used across government. The process will employ common data elements that can be easily shared and integrated into the respective organization's database for shared or unique analysis efforts.

Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive. FedCIRC, the NIPC, the NSIRC, the Department of Defense and industry components realize that the best response is a preemptive and proactive approach. In order to implement such an approach, all resources must be focused on the common goal of securing the nation's critical infrastructures and the strengths of each organization must be relied upon in order to achieve the most ef-

fective results. FedCIRC, the NIPC, DOD, the NSIRC and others comprise a virtual team, each offering significant skills and contributions to the common defense.

SUMMARY

Madam Chairwoman, the information presented today highlights the high degree of cooperation among government agencies and the critical and effective relationship that exists between FedCIRC and the NIPC. Though all contribute individually to critical infrastructure protection, our strength in protecting information systems government-wide lies in collaboration and coordination efforts. I trust that you will derive from my remarks an understanding of the cyber-threat and response issues and also an appreciation for the joint commitment to infrastructure protection of FedCIRC and the NIPC. We appreciate your leadership and that of the Committee for helping us achieve our goals and allowing us to share information that we feel is crucial to the defense of our technology resources.

Chairperson FEINSTEIN. Thanks very much, Ms. McDonald.

Mr. Savage, of the Secret Service.

STATEMENT OF JAMES A. SAVAGE, JR., DEPUTY SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE, WASHINGTON, D.C.

Mr. SAVAGE. Madam Chairman, Ranking Member Kyl, thank you for the opportunity to address the Subcommittee regarding the efforts of the Secret Service as they relate to the protection of our Nation's critical infrastructures. I have prepared a comprehensive statement which will be submitted for the record, and with the Subcommittee's permission I will summarize it at this time.

I am particularly pleased to be here with my colleagues and partners in fighting cyber crime from the FBI, GSA, and the private sector. The Secret Service contributes to the protection of our Nation's critical infrastructures through its fight against cyber crime as part of our core mission to protect the integrity of this Nation's financial payment systems and the telecommunications backbone.

Since our inception in 1865 with an initial mandate to suppress the counterfeiting of currency, modes and methods of payment have evolved and so has our mission. Computers and other chip devices are now the facilitators of criminal activity or the target of such. In this era of change, one constant that remains is our close working relationship with the banking and finance sector. We believe that protection of the banking and financial infrastructures is our core competency area.

Madam Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial infrastructures. There is, however, a scarcity of information regarding successful models to combat this crime in today's high-tech environment. That is where the Secret Service can make a significant contribution to today's and future discussions of successful law enforcement efforts to combat cyber crime.

The Secret Service has developed a highly effective formula for combatting high-tech crime, as demonstrated by our New York Electronic Crimes Task Force. This task force, hosted by the Secret Service, includes 50 different law enforcement agencies, over 100 private sector corporations and six different universities. The notion of these companies, these competitors, and 100 others sitting down at the same table to share information, knowledge and resources with both each other and with law enforcement is why we

believe we have found a truly unique, innovative and effective formula for combatting cyber crime. The task force provides a collaborative crime-fighting environment which reflects our recognition that in today's high-tech electronic crime environment, out-of-the-box problems demand out-of-the-box solutions.

How effective has this task force been? Since 1995, the New York Task Force has charged over 800 individuals with electronic crimes valued at more than $425 million. It has trained over 10,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them.

Based on the enormous success of this task force, the Secret Service hopes to replicate the model and concepts developed by our New York field office in additional venues around the country in the very near future. The Secret Service believes there is value in sharing information from our investigations and the lessons we learn along the way with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. Law enforcement must move from a reactive posture to a proactive or preventive posture by helping its customers to help themselves.

The hallmark qualities of discretion and trust which we employ in the execution of our protective duties are also present in our investigative mission, where we enjoy quiet successes with our private sector partners. We have jointly resolved many significant cases with the help of our private sector counterparts, such as network intrusions and compromises of critical information systems.

The Secret Service recognizes that its role in investigating computer-based attacks against the financial sector can be significant in the larger plan for the protection of our Nation's critical infrastructures. When we share helpful prevention strategies with a business seeking to protect itself, or arrest a criminal who has disrupted a sensitive communications network and are able to restore the normal operation of the host, be it a bank, telecommunications carrier or medical service provider, we believe we have made a significant contribution toward assuring the reliability of the critical systems that the public relies upon on a daily basis.

The Secret Service is convinced that building trusted partnerships with the private sector, local law enforcement, and academia is the model for combatting electronic crimes in the information age.

Madam Chairman, that concludes my prepared statement. I will be happy to answer any questions that you or the other members may have. Thank you.

[The prepared statement of Mr. Savage follows:]

STATEMENT OF JAMES A. SAVAGE, JR., DEPUTY SPECIAL AGENT IN CHARGE-FINANCIAL CRIMES DIVISION

Madam Chairman, members of the subcommittee, thank you for the opportunity to address the subcommittee regarding federal law enforcement efforts in combating cyber crime to protect our nation's infrastructures, and particularly the efforts of the Secret Service in this regard. I am particularly pleased to be here with my colleagues and partners in fighting cyber crime from the Federal Bureau of Investigation and the General Services Administration.

As you know, the Secret Service was created in 1865 to address the burgeoning problem of counterfeit currency. At that time, it was estimated that approximately

one third of all currency in circulation was counterfeit and the government recognized the urgent need to address this issue in order to maintain the public's confidence in the U.S. currency. In effect, the Secret Service was engaged in an effort to protect a critical governmental function long before the popular notion of critical infrastructure protection emerged.

Today, the Secret Service continues to suppress counterfeit currency as part of its traditional role but also now includes fighting cyber crime as part of our core mission to protect the integrity of this nation's financial payment systems. Over time, modes and methods of payment have evolved and so has our mission. Computers and other "chip" devices are now the facilitators of criminal activity or the target of such. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals—all of whom recognize new opportunities and anonymous methods to expand and diversify their criminal portfolio.

In this era of change, one constant that remains is our close working relationship with the banking and finance sector. Our history of cooperation with the industry is a result of our unique responsibilities as a law enforcement bureau of the Department of the Treasury. We believe that protection of the banking and financial infrastructure is our "core competency" area.

Madam Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial infrastructures and the need to create effective solutions. There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment. That is where the Secret Service can make a significant contribution to today's and future discussions of successful law enforcement efforts to combat cyber crime which play an important role in critical infrastructure protection.

The Secret Service has found a highly effective formula for combating high tech crime a formula that has been successfully developed by our New York Electronic Crimes Task Force. While the Secret Service leads this innovative effort, we do not control or dominate the participants and the investigative agenda of the task force. Rather, the task force provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

Although based in New York City, the task force provides assistance and conducts investigations, which span the country and often lead overseas, harnessing disparate repositories of resources and expertise from the academic, private and government sectors. It is not uncommon for the New York Task Force to receive requests for assistance directly from foreign law enforcement representatives based upon its reputation for responsiveness and as a center of excellence. The result is a significant impact domestically, and occasionally abroad, as well.

Within this New York model, established in 1995, there are 50 different federal, state and local law enforcement agencies represented as well as prosecutors, academic leaders and over 100 different private sector corporations. The wealth of expertise and resources that reside in this task force coupled with unprecedented information sharing yields a highly mobile and responsive machine. In task force investigations, local law enforcement officers hold supervisory positions and representatives from other agencies regularly assume the role of lead investigator. These investigations encompass a wide range of computer-based criminal activity, involving e-commerce frauds, intellectual property violations, telecommunications fraud, and a wide variety of computer intrusion crimes, which affect a variety of infrastructures.

Since 1995, the task force has charged over 800 individuals with electronic crimes valued at more than $425 million. It has trained over 10,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. We view the New York Electronic Crimes Task Force as the model for the partnership approach that we hope to employ in additional venues around the country in the very near future.

An important component in our investigative response to cyber crime and critical infrastructure protection is the Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training in forensic identification, preservation, and retrieval of electronically stored evidence. Special Agents entering the program receive specialized training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers,

personal data assistants, telecommunications devices, electronic organizers, scanners, and other electronic paraphernalia. ECSAP agents understand that not only do they have an investigative role, and that they can also help protect components of our critical infrastructure by providing their substantive insights regarding potential vulnerabilities and exploits which the Secret Service discovers during an investigation.

As a specific example, in early August we will be meeting with representatives of a major financial group, which is in the process of developing its own computer forensic capability to bolster its defenses against internal and external computer based frauds and attacks. We hope to share with this prominent corporation the lessons we have learned in establishing and maintaining our ECSAP computer forensics program as well as explore areas for joint endeavors in the future.

The Secret Service ECSAP program relies on the 4 year-old, Treasury-wide Computer Investigative Specialist (CIS) initiative. All four Treasury law enforcement bureaus—the Internal Revenue Service, Bureau of Alcohol, Tobacco and Firearms, U.S. Customs Service, and the U.S. Secret Service—participate and receive training and equipment under this program.

All four Treasury bureaus also jointly participate in curriculum development and review, equipment design and distribution of training assets. As a result, financial savings by all Treasury bureaus are realized due to economies of scale. Additionally, agents from different bureaus can work together in the field in an operational capacity due to the compatibility of the equipment and training. In the end, the criminal element suffers and the taxpayer benefits.

The Secret Service works cooperatively with other federal law enforcement and Department of Defense agencies in this work, to include the FBI and NIPC. No single agency or entity can prevent cybercrime or protect the critical infrastructure alone, so Secret Service agents work collaboratively with their peers in the field to investigate crimes and overcome technical problems. I would further add, Madam Chairman, that due to the proliferation and complexity of cyber crime there is certainly no shortage of opportunity to collaborate with our other Federal partners in this regard.

Because of the recognized expertise of those in ECSAP, other law enforcement agencies regularly request training from the Secret Service or advice concerning their own computer forensics programs. These requests have come from agencies all across the country, as well as foreign countries such as Italy and Thailand. The Secret Service recognizes the need to promote international cooperation and remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, regarding program initiatives and current financial and electronic crimes trends.

Madam Chairman, we are committed to working closely with our law enforcement counterparts worldwide in response to cyber crime threats to commerce and financial payment systems. This commitment is demonstrated by our effort to expand our overseas presence. We currently have 18 offices in foreign countries and a permanent assignment at Interpol, as well as several overseas initiatives, including a cyber crime task force in Indonesia. New offices have been opened recently in Frankfurt, Lagos, and Mexico City. The Secret Service is also considering opening new offices in Bucharest and New Dehli. Our expanded foreign presence increases our ability to become involved in foreign investigations that are of significant strategic interest.

In addition to providing law enforcement with the necessary technical training and resources, a great deal more can be accomplished in fighting cyber crime if we are able to harness additional resources that exist from the private sector and academia. The Secret Service believes there is value in sharing information during the course of our investigations with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. On occasion the Secret Service has shared case-specific information derived from our criminal investigations after taking appropriate steps to protect privacy concerns and ensure that there are no conflicts with prosecutorial issues. I would add that there are many opportunities for the law enforcement community to share information with our private sector counterparts without fear of compromise. The Secret Service recognizes the need for a "paradigm shift" with respect to this type of information sharing between law enforcement and our private sector and academic counterparts.

Finally, law enforcement in general is not sufficiently equipped to train all those in need nor can it compete with academic institutions of higher learning in the area of research and development. However, our partnerships with industry and academia have demonstrated that this should be an integral part of the solution.

Partnership concepts are an important tool and strategy in both government and private industry to achieve greater results and efficiencies. Unfortunately, however, partnerships cannot be legislated, regulated, or stipulated. Nor can partnerships be purchased, traded or incorporated. Partnerships are built between people and organizations that recognize the value in joint collaboration toward a common end. They are fragile entities, which need to be established and maintained by all participants and built upon a foundation of trust.

The Secret Service, by virtue of the protective mission for which we are so well known, has always emphasized discretion and trust in executing our protective duties. We learned long ago that our agency needed the full support and confidence of local law enforcement and certain key elements of the private sector to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we need to maintain a trusted relationship with our protectees so that we can work with them and their staffs to maintain the delicate balance between security and personal privacy.

This predisposition towards discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners. We have successfully investigated many significant cases with the help of our private sector partners such as network intrusions and compromises of critical information or operating systems. In such cases, even though we have technical expertise that is second to none, we still rely on our private sector counterparts to collaborate with us in identifying and preserving critical evidence to solve the case and bring the perpetrator to justice. Equally important in such cases is conducting the investigation in a manner that avoids unnecessary disruption or adverse consequences to the victim or business. With the variety of operating platforms and proprietary operating systems in the private sector, we could not accomplish these objectives without the direct support of our private sector counterparts.

I would like to highlight several significant cases that the Secret Service has investigated over the years where we have protected the U.S. financial and telecommunications systems.

In 1986, the USSS identified and prosecuted the "Legion of Doom" hacker group for compromising the 911 system in the southeast United States.

In 1989, the USSS, working with the FBI and other law enforcement entities, identified and prosecuted the "Masters of Deception" hacker group which had compromised several communications networks in the U.S. enabling the group to identify and reveal the details concerning on-going law enforcement wiretaps.

In 1994, the USSS conducted the first e-mail wiretap ever conducted on the Internet as part of a telecommunications fraud investigation.

In 1997, the US–SS identified and arrested a hacker responsible for compromising a telephone network switch on the east coast, effectively disabling power and communications to the Worcester, MA. Airport. This resulted in the first prosecution of a juvenile for violation of 18 USC 1030.

In 1998, the USSS and its task force partners in New York, identified and arrested individuals who were illegally monitoring law enforcement Mobile Data Terminals.

Madam Chairman, the USSS continues to remain engaged in these types of significant investigations, which not only involve notable financial losses, but also represent the exploitation of technical vulnerabilities in and amongst interconnected computer-based systems which support our critical infrastructures. Of particular note is that such cases necessarily require a close working relationship with the private sector victim to achieve success.

In fact, in one recently completed complex investigation involving the compromise of a wireless communications carrier's network, our case agent actually specified in the affidavit of the federal search warrant that representatives of the victim business be allowed to accompany federal agents in the search of the target residence to provide technical assistance. This is unprecedented in the law enforcement arena and underscores the level of trust we enjoy with those we have built relationships with in the private sector. It is also indicative of the complexity of many of these investigations and serves to highlight the fact that we in law enforcement must work with private industry to be an effective crime fighting force. In approving this search warrant, the court recognized that in certain cases involving extraordinarily complex systems and networks, such additional technical expertise could be a critical, and sometimes imperative, component of our investigative efforts.

I must point out, however, that such cases are usually not publicized without the express consent of the U.S. Attorney and the corporate victim because it would breach our confidential relationship and discourage the victims of electronic crimes from reporting such incidents.

Four recently concluded investigations demonstrate the breadth of cases the Secret Service is working, and provide concrete evidence of the continuing success of ECSAP. The cases include the malicious shutdown of a medical service provider's communications system, an intrusion into a telecommunication provider's network, an attack on a private investment company's trading network, and the disruption of a financial institution's complete operating system and communications network.

The first case was initiated on March 5, 2001, when a local Secret Service field office received information that a medical diagnostic service provider had suffered a catastrophic shutdown of its computer network and communications system. The company reported that they were unable to access doctor schedules, diagnostic images, patient information, and essential hospital records, which adversely affected their ability to provide care to patients and assist dependent medical facilities.

Within a matter of hours, a Secret Service ECSAP agent was able to regain control of the network by coordinating with the facility's system administrator to temporarily shutdown and reconfigure the computer system. The ECSAP agent also essentially "hacked" into the compromised system, and modified compromised password files to "lock out" the attacker. This was accomplished while maintaining control of the computer system log files containing evidence of how the intrusion had occurred.

Using this evidence, a federal search warrant was obtained for the residence of a former employee of the hospital, who had recently been terminated from his position as system administrator. Computer equipment was seized pursuant to the warrant, the suspect admitted to his involvement, and federal computer fraud charges are pending.

A case with obvious critical infrastructure implications was initiated on February 20, 2001, when two major wireless telecommunications service providers notified the New York Electronic Crimes Task Force that they had identified two hackers in different remote sites who were attacking their systems. These hackers were manipulating the systems to obtain free long distance service, re-route numbers, add calling features, forward telephone numbers, and install software that would ensure their continued unauthorized access.

The level of access obtained by the hackers was virtually unlimited, and had they chosen to do so, they could have shut down telephone service over a large geographic area, including "911" systems, as well as service to government installations and other critical infrastructure components.

On March 20, 2001, the Secret Service simultaneously executed search warrants in New York City and Phoenix and computer equipment was seized at both locations. One suspect was arrested on federal computer fraud charges, while the other suspect was questioned and released pending a decision by the Department of Justice as to whether or not to pursue federal charges.

The third case occurred from March 9, 2000, through March 14, 2000, when a company located in New York, NY, received several Internet-based "denial of service" attacks on its servers. A "denial of service" attack occurs when a perpetrator launches malicious programs, information, codes, or commands to a target or victim computer which causes it to shut down, thereby denying access by legitimate customers to those computers. In this instance, the company was a prominent provider of electronic trading services on Wall Street.

While the attacks were still occurring, the company's CEO contacted the Secret Service's New York Electronic Crimes Task Force. The CEO identified a former employee as a suspect, based upon the fact that the attacks preyed on vulnerabilities, which would only be known to the former employee. These attacks continued through March 13, 2000, when ECSAP agents and task force members identified the attacking computer and arrested the former employee for violating Title 18, USC, Section 1030 (Computer Fraud). In a post-arrest statement, the suspect admitted that he was responsible for the denial of service attacks. As a result of the attacks, the company and its customers lost access to trading systems. Approximately $3.5 million was identified in lost trading fees, commissions, and liability as a result of the customers' inability to conduct any trading.

The last case began just last month when a financial institution notified local police who in turn notified the local office of the Secret Service, that its entire banking and communications network had been shut down. The institution reported that it was severely crippled, as it had no access to electronic data used in support of its ATMs, banking transactions, employee payroll and all other critical functions. Working with the local police and the bank's technical staff, a former employee emerged as a suspect and electronic evidence was developed that strongly indicated his involvement. During an ensuing interview with agents and police, the suspect admitted to disabling the bank's system and "hacking" an unrelated database in his attempts to exact revenge upon the bank CEO. Federal charges are pending.

Let me emphasize the Secret Service's mission in fighting cyber crime as it relates to the bigger picture of critical infrastructure protection. As previously stated, we target cyber crime as it may affect the integrity of our nation's financial payment and banking systems. As we all know, the banking and finance sector comprises a very critical infrastructure sector and one, which we have historically protected and will continue to protect. In this context, our efforts to combat cyber assaults, which target information, and communication systems, which support the financial sector, are parts of the larger and more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected. To put this all in perspective, the public's confidence is lost if such delivery systems and services are unreliable, unavailable, or unpredictable regardless of the cause of the problem.

We also recognize that our unique protective responsibilities, including our duties as the lead federal agency for coordinating security at National Special Security Events, demand heightened electronic security awareness and preparation. A well-placed cyber attack against a weak technology or support infrastructure system can render an otherwise sound physical security plan vulnerable and inadequate.

To further advance our efforts in this regard, the Secret Service will soon commence a significant collaborative project with the Software Engineering Institute (SEI) at Carnegie Mellon University which has operated the Computer Emergency Response Team (CERT) Coordination Center since 1988. Jointly, the Secret Service and the SEI plan to combine expertise in developing strategies and programs to effectively address cyber threats, which may impact our protective and investigative missions.

Madam Chairman, it should also be noted that all deliberate infrastructure attacks, before they rise to such a threshold, are also cyber crimes and are likely to be dealt with initially by law enforcement personnel, both federal and local, in the course of routine business. In fact, I don't believe there is universal agreement as to when a "hack" or network intrusion rises to the threshold of an infrastructure attack and corresponding national security event but we would all probably recognize one when it reached catastrophic proportions.

Given this continuum and interplay between computer-based crimes and national security issues, the Secret Service recognizes that its role in investigating and helping to prevent computer-based attacks against the financial sector can be significant in the larger plan for the protection of our nation's critical infrastructures. When we arrest a criminal who has breached and disrupted a sensitive communications network and are able to restore the normal operation of the host—be it a bank, telecommunications carrier, or medical service provider—we believe we have made a significant contribution towards assuring the reliability of the critical systems that the public relies upon on a daily basis. But greater satisfaction and success are achieved when a potentially devastating incident is prevented due to our prior involvement, participation, or sharing of information.

As a footnote, the Secret Service met recently with representatives of the Financial Services Information Sharing and Analysis Center (FS/ISAC) that was created pursuant to Presidential Decision Directive (PDD) 63. The directive mandated the Department of the Treasury to work with members of the banking and finance sector to enhance the security of the sector's information systems and other infrastructures, a responsibility managed by Treasury's Assistant Secretary of Financial Institutions. The role of the FS/ISAC is to devise a way to share information within the financial services industry relating to cyber threats and vulnerabilities. The Secret Service feels that it can make a significant contribution to the work of the FS/ISAC and is exploring common areas of interest with the FS/ISAC, to include information sharing.

The Secret Service continues to receive requests from local law enforcement agencies and others for assistance, and we welcome those requests. On an increasing basis, our local field offices and the Financial Crimes Division of the Secret Service receive desperate pleas from local police departments for physical assistance, training and equipment in the area of computer forensics and electronic crimes so that they can continue to provide a professional level of service and protection for their citizens. The Secret Service has become an important option for local law enforcement, the private sector and others to turn to when confronted with network intrusions and other sophisticated electronic crimes.

Over the past 3 years, Secret Service ECSAP agents completed 2,122 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams done for other law enforcement agencies during this period, it is estimated that some 10 to 15 percent of these examinations fell in this category. Many of the examinations were conducted in support of other agen-

cies' investigations such as those involving child pornography or homicide cases simply because the requesting agency did not have the resources to complete the examination itself.

We do provide assistance on a regular basis to other departments, often sending ECSAP agents overnight to the requesting venue to perform computer related analyses or technical consultation. In fact, so critical was the need for even basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the line officer and detective alike. Madam Chairman, with your permission, I would like to submit a copy of this guide for the record.

We have also worked with this group to produce the interactive, computer-based training program known as "Forward Edge" which takes the next step in training officers to conduct electronic crime investigations. Forward Edge incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the two-CD training program and are immediately accessible for instant implementation.

Thus far we have dispensed over 220,000 "Best Practices Guides" to local and federal law enforcement officers and we will soon distribute, free of charge, over 20,000 Forward Edge training CDs.

In an additional effort to further enhance information sharing between the law enforcement community and the financial industry, the Secret Service recently created the "E Library" Internet website which serves as a mechanism for all members to post specific information, images and alerts relating to fictitious financial instruments, counterfeit checks, and credit card skimming devices. This website is accessible free of charge to all members of the law enforcement and banking communities and is the only such tool of its kind.

In today's high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration amongst the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that building trusted partnerships with the private sector and its Federal and local law enforcement partners is the model for combating electronic crimes in the information age.

Madam Chairman, that concludes my prepared statement, and I would be happy to answer any questions that you or other members of the subcommittee may have.

ADDITIONAL STATEMENT OF JAMES A. SAVAGE, JR., DEPUTY SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE

PLEASE PROVIDE A SUMMARY OF THE SECRET SERVICE'S EFFORTS TO PROVIDE TRAINING TO OTHER LAW ENFORCEMENT AGENCIES——

Because of the increased importance of electronic evidence in all types of criminal investigations, the demand for timely examinations of seized electronic media by well-qualified computer investigative specialists has skyrocketed during the past few years. Many state and local law enforcement agencies do not have the necessary resources or expertise to fully develop their own computer forensic programs, and are having difficulty keeping up with requests for examinations from their own officers and investigators. Secret Service personnel in the Electronic Crimes Special Agent Program (ECSAP) have provided timely assistance to such agencies with respect to counterfeit, financial and electronic crimes investigations. However, providing ECSAP support in a timely manner is becoming increasingly challenging in light of the rapidly escalating number of requests.

In an effort to assist state and local law enforcement agencies improve their own computer forensic capabilities, the Secret Service has recently sponsored the attendance of a limited number of state and local officers and investigators at the six-week Basic Computer Evidence and Recovery Training (BCERT) course. This training program is identical to the initial training provided to those in ECSAP. The Secret Service has also developed a two-week Basic Computer Forensics (BCF) course exclusively for state and local officers and investigators that will be taught by Secret Service ECSAP personnel and outside vendors. The first BCF course, which is being offered at no cost to the 12 attendees, is scheduled for September 17–28, 2001.

Other law enforcement agencies regularly request training from the Secret Service regarding financial and electronic crime trends and investigative methodologies, as well as advice concerning their own computer forensics programs. These requests have come from agencies all across the country, as well as from foreign countries in Asia and Europe. The Secret Service remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, with respect to program initiatives and current trends and schemes through a variety of partnerships and initiatives.

In conjunction with the International Association of Chiefs of Police (IACP), the Secret Service developed the "Best Practices for Seizing Electronic Evidence Manual", to assist law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies. The demand for the "Best Practices" guide has been so great that the supply from each of the first four printings, totaling over 220,000 copies, was exhausted literally within days.

As a follow-up to the "Best Practices" guide, the Secret Service and the IACP produced the interactive, computer-based training program known as "Forward Edge" which takes the next step in training officers to conduct electronic crime investigations. Forward Edge incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the two-CD training program and are immediately accessible for instant implementation.

In an additional effort to further enhance information sharing between the law enforcement community and the financial industry, the Secret Service recently created the "eLibrary" Internet website which serves as a mechanism for all members to post specific information, images and alerts relating to fictitious financial instruments, counterfeit checks, and credit card skimming devices. This website is accessible free of charge to all members of the law enforcement and banking communities and is the only such tool of its kind.

In December of 2000, the Secret Service coordinated an Identity Theft Workshop in Washington, D.C. This workshop was designed for the criminal investigator and was attended by investigators from agencies throughout the nation. The workshop provided investigators with a detailed explanation of how identity theft can occur, as well as an explanation of what tools are available to investigators.

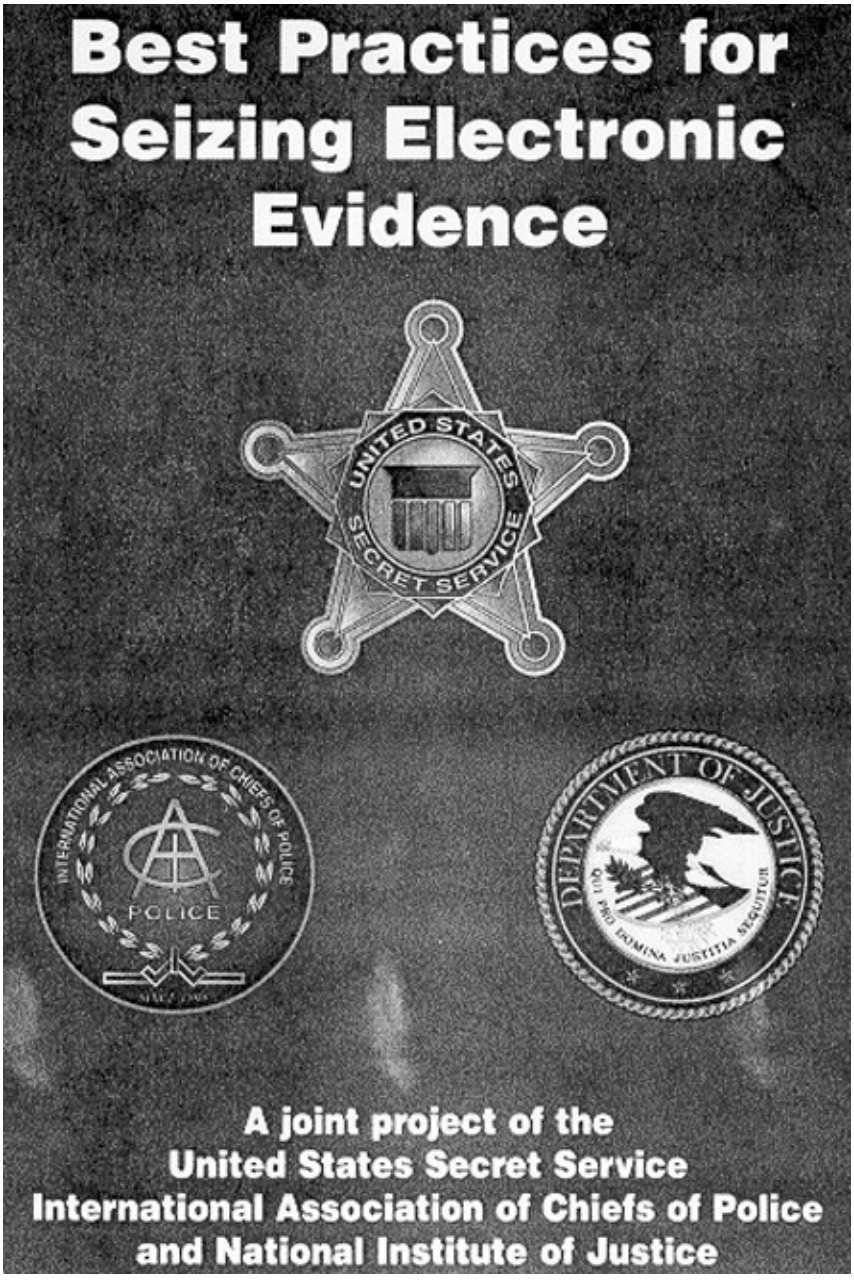
In May of 2001, the Secret Service made an identity theft presentation to the IACP Advisory Committee for Police Investigation Operations. During this presentation, the Secret Service proposed the production of an identity theft video geared toward police officers throughout the nation. The purpose of this video will be to emphasize the need for police to document a citizen's complaint of identity theft, regardless of the location of the suspects (if any). In addition, the video and its companion reference card will provide officers with phone numbers that can assist victims. The Advisory Committee is supportive of this effort, and is considering providing funding for it, and pursuing it jointly with the Secret Service, as was done with the "Best Practices" initiative.

To emphasize the philosophy that financial and electronic crimes investigations are routinely international in scope, and to demonstrate the commitment of the Secret Service to strengthening investigative efforts and liaison with foreign law enforcement entities, representatives of the Secret Service have participated in briefings and provided instruction to over twenty different foreign law enforcement groups both in Washington, D.C. and at overseas locations around the world. Highlights include:

Developing the curriculum for a two-week specialized course titled "Combating Counterfeit and Financial Crimes in the New Millennium" that was taught by Secret Service instructors at the Bangkok International Law Enforcement Academy to a class of more than thirty command-level law enforcement officials from ten different countries;

Sending two different delegations to Rome, Italy, to give briefings to the Guardia di Finanza regarding electronic crimes initiatives and computer forensics issues, as well as hosting two visits by Italian delegations to the Secret Service Financial Crimes Division; and

Having a Secret Service Special Agent spend two weeks in Bangkok, Thailand, working with law enforcement officials and industry representatives to address means of combating Thailand's rampant cellular telephone fraud, including correcting systemic weaknesses and developing cellular telephone tracking and mapping techniques.


Best Practices for Seizing Electronic Evidence
UNITED STATES SECRET SERVICE
INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
POLICE
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
A joint project of the
United States Secret Service
International Association of Chiefs of Police
and National Institute of Justice

The *Best Practices for Seizing Electronic Evidence* was developed as a project of the International Association of Chiefs of Police Advisory Committee for Police Investigative Operations. The Committee convened a working group of a variety of law enforcement representatives, facilitated by the United States Secret Service, to identify common issues encountered in today's crime scenes. This manual was developed by representatives from the following agencies:

Alexandria, Virginia Police Department
Boston, Massachusetts Police Department
Baltimore County Police Department
Clarkstown, New York Police Department
Department of Justice – Computer Crimes and Intellectual Property Section
Florida Department of Law Enforcement
Florida Statewide Prosecutors Office
High Intensity Drug Trafficking Area (HIDTA) Program
Los Angeles County District Attorneys Office
Los Angeles Police Department
Lubbock, Texas Police Department
Maryland Heights, Missouri Police Department
National Association of Attorneys General
National Institute of Justice
National Sheriffs Association
New Jersey Division of Criminal Justice
New York City Police Department
New York County District Attorneys Office
New York State Organized Crime Task Force
Provo, Utah Police Department
Richardson, Texas Police Department
Rockland County New York District Attorneys Office
St. Louis County Police Department
United States Secret Service
Utah County Attorneys Office

Feedback!

If you have comment on this manual, please send it via email to
iacp_manual@usss.treas.gov

Best Practices for Seizing Electronic Evidence

Purpose

To develop a basic understanding of key technical and legal factors regarding searching and seizing electronic storage devices and media.

Introduction

Scope of the Problem

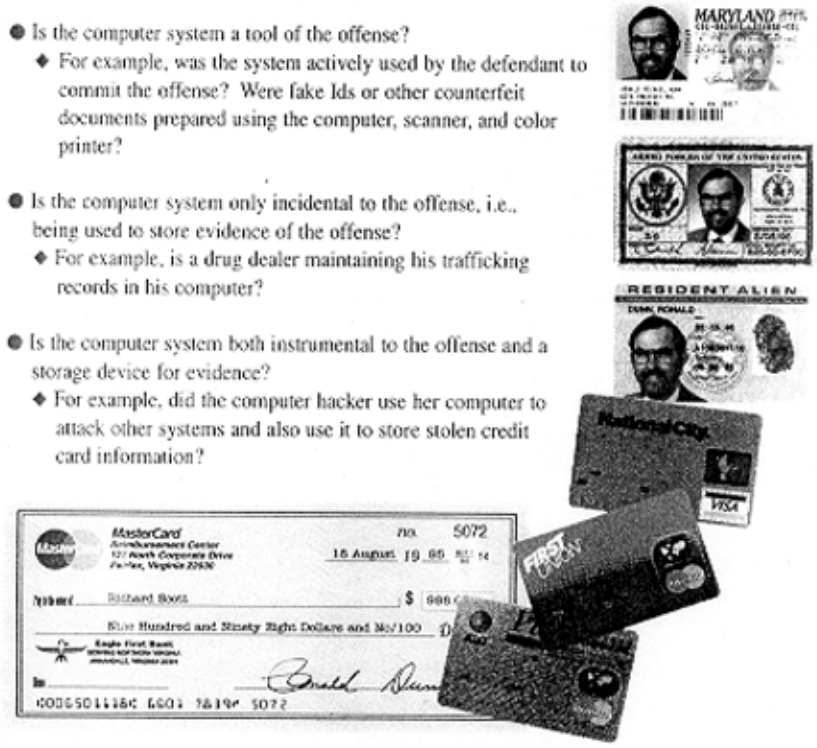
As computers and related storage and communication devices proliferate in our society, so does the use of those devices in conducting criminal activities. Technology is employed by criminals as a means of communication, a tool for theft and extortion, and a repository to hide incriminating evidence or contraband materials. Law enforcement officers must possess up-to-date knowledge and equipment to effectively investigate today's criminal activity. The law enforcement community is challenged by the task of identifying, investigating and prosecuting individuals and organizations that use these and other emerging technologies to support their illicit operations.

Recognizing Potential Evidence

Computers and digital media are increasingly involved in unlawful activities. The computer may be contraband, fruits of the crime, a tool of the offense, or a storage container holding evidence of the offense. Investigation of any criminal activity may produce electronic evidence. Computers and related evidence range from the mainframe computer to the pocket-sized personal data assistant to the floppy diskette, CD or the smallest electronic chip device. Images, audio, text and other data on these media are easily altered or destroyed. It is imperative that law enforcement officers recognize, protect, seize and search such devices in accordance with applicable statutes, policies and best practices and guidelines.

Answers to the following questions will better determine the role of the computer in the crime:

- Is the computer contraband or fruits of a crime?
  - For example, was the computer software or hardware stolen?
- Is the computer system a tool of the offense?
  - For example, was the system actively used by the defendant to commit the offense? Were fake Ids or other counterfeit documents prepared using the computer, scanner, and color printer?
- Is the computer system only incidental to the offense, i.e., being used to store evidence of the offense?
  - For example, is a drug dealer maintaining his trafficking records in his computer?
- Is the computer system both instrumental to the offense and a storage device for evidence?
  - For example, did the computer hacker use her computer to attack other systems and also use it to store stolen credit card information?



Once the computer's role is understood, the following essential questions should be answered:

- Is there probable cause to seize hardware?
- Is there probable cause to seize software?
- Is there probable cause to seize data?
- Where will this search be conducted?
  - For example, is it practical to search the computer system on site or must the examination be conducted at a field office or lab?
  - If law enforcement officers remove the system from the premises to conduct the search, must they return the computer system, or copies of the seized data, to its owner/user before trial?
  - Considering the incredible storage capacities of computers, how will experts search this data in an efficient, timely manner?

Preparing For The Search And/Or Seizure

Using evidence obtained from a computer in a legal proceeding requires:

- Probable cause for issuance of a warrant or an exception to the warrant requirement.
  - Caution: If you encounter potential evidence that may be outside the scope of your existing warrant or legal authority, contact your agency's legal advisor or prosecutor as an additional warrant may be necessary.
- Use of appropriate collection techniques so as not to alter or destroy evidence.
- Forensic examination of the system completed by trained personnel in a speedy fashion, with expert testimony available at trial.

Conducting The Search And/Or Seizure

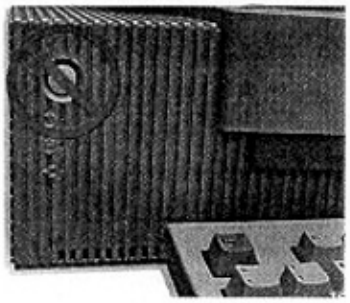
Once The Computer's Role Is Understood And Legal Requirements Are Fulfilled:

1. Secure The Scene

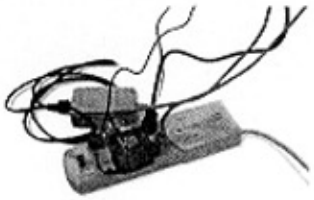
- Officer Safety is Paramount.
- Preserve Area for Potential Fingerprints.
- Immediately Restrict Access to Computer(s).
  - Isolate from Phone Lines. (Because data on the computer can be accessed remotely.)

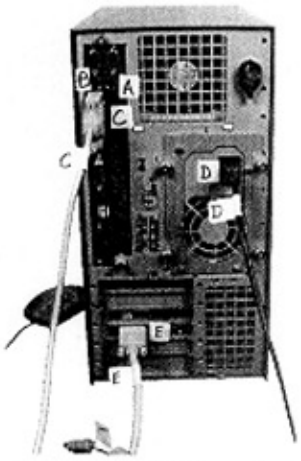
2. Secure The Computer As Evidence

- If Computer is "OFF," DO NOT TURN "ON"



- If Computer is "ON"
  - Stand-Alone Computer (Non-Networked)
    - Consult Computer Specialist





  - If Specialist is Not Available
    - Photograph screen, then disconnect all power sources; unplug from the wall **AND** the back of the computer.
    - Place evidence tape over each drive slot.
    - Photograph/diagram & label back of computer components with existing connections.
    - Label all connectors/cable ends to allow reassembly as needed.
    - If transport is required, package components and transport/store components as fragile cargo.
    - Keep away from magnets, radio transmitters and otherwise hostile environments.

Networked Or Business Computers

Consult A Computer Specialist For Further Assistance

▼ Pulling the plug could:

- Severely damage the system
- Disrupt legitimate business
- Create officer and department liability

Other Electronic Storage Devices

Electronic devices may contain viable evidence associated with criminal activity. Unless an emergency exists, the device should not be accessed. Should it be necessary to access the device, all actions associated with the manipulation of the device should be noted in order to document the chain of custody and insure its admission in court.

I. Wireless Telephones

● Potential Evidence Contained In Wireless Devices

- ◆ Numbers called
- ◆ Numbers stored for speed dial
- ◆ Caller ID for incoming calls
- ◆ Other information contained in the memory of wireless telephones
  - ✦ Phone/pager numbers
  - ✦ Names and addresses
  - ✦ PIN numbers
  - ✦ Voice mail access number
  - ✦ Voice mail password
  - ✦ Debit card numbers
  - ✦ Calling card numbers
  - ✦ E-mail/Internet access information
  - ✦ The on screen image may contain other valuable information

● On/Off Rule

- ◆ If the device is "ON", do NOT turn it "OFF"
  - ✦ Turning it "OFF" could activate lockout feature
  - ✦ Write down all information on display (photograph if possible)
  - ✦ Power down prior to transport (Take any power supply cords present)
- ◆ If the device is "OFF", leave it "OFF"
  - ✦ Turning it on could alter evidence on device (Same as computers)
  - ✦ Upon seizure get it to an expert as soon as possible or contact local service provider
  - ✦ If an expert is unavailable, USE A DIFFERENT TELEPHONE and contact 1800-LAWBUST (a 24 x 7 service provided by the cellular telephone industry)

II. Electronic Paging Devices

- **Potential Evidence Contained in Paging Devices**
  - Numeric Pagers receives only numeric digits (can be used to communicate numbers and code)
  - Alpha Numeric Pagers (receives numbers and letters and can carry full text)
  - Voice Pagers (can transmit voice communications (sometimes in addition to alpha numeric)
  - 2-way pagers (Containing incoming and outgoing messages)
  - Best Practices
    - Once pager is no longer in proximity to suspect - turn it off. Continued access to electronic communications over pager without proper authorization can be construed as unlawful interception of electronic communication
  - Search of stored contents of pager
    - Incident to Arrest
    - With probable cause + exception
    - With consent

III. Facsimile Machines

- **Fax machines can contain:**
  - Speed dial lists
  - Stored faxes (incoming and outgoing)
  - Fax transmission logs (incoming and outgoing)
  - Header line
  - Clock setting

- **Best Practices - Fax Machines**
  - If fax machine is found "ON"
    - Powering down may cause loss of last number dialed and/or stored faxes

- **Other Considerations**
  - Search Issues
    - Record telephone line number fax is plugged into
    - Header line should be the same as the phone line . . .user sets header line
    - All manuals should be seized with equipment, if possible

IV. Caller ID Devices

- May contain telephone and subscriber information from incoming telephone calls
  - Interruption of the power supply to the device may cause loss of data if not protected by internal battery back up
    - Document all stored data prior to seizure or loss of data may occur

V. Smart Cards: A plastic card the size of a standard credit card that holds a microprocessor (chip) which is capable of storing monetary value and other information.

- **Awareness**
  - Physical characteristics of the card
  - Photograph of the smart card
    - Label and identify characteristics
    - Features similar to credit card/driver's license
    - Detect possible alteration or tampering during same examination

- **Uses of Smart Card**
  - Point of sale transactions
  - Direct exchange of value between cardholders
  - Exchange of value over the Internet
  - ATM capabilities
  - Capable of storing other data and files similar to a computer

- Same as credit cards
- Numerous cards, (different names or same issuing vendor)
- Signs of tampering
  - Cards are found in the presence of computer or other electronic devices

Questions to Ask When Encountering Smart Cards

- Who is card issued to (the valid cardholder)?
- Who issued the card?
- What are the uses of the cards?
- Why does the person have numerous cards?
- Can this computer or device alter the card?

Other Considerations

- Smart Card technology is used in some cellular phones and may be found in or with cellular devices(See Wireless Section)

Tracing an Internet Email

- When an internet e-mail message is sent, the user typically controls only the recipient line(s) (To: and Bcc:) and the Subject: line.
- Mail software adds the rest of the header information as it is processed.

Reading an email header:

Sample Email Header

```
                    - - - - - Message header follows - - - - -
(1) Return-path: <ambottom@ol67832.cc.nps.navy.mil>
(2) Received: from ol67832.cc.army.mil by nps.navy.mil
    (4.1/SMI-4.1) id AA08660; Thur, 7 Nov 96 17:51:49 PST
(3) Received: from localhost byol67832.navy.mil (4.1/SMI-4.1)
    id AA16514; Thur, 7 Nov 96 17:50:53 PST
(4) Message-Id: <9611080150.AA16514@ol67832.cc.army.mil>
(5) Date: ThuI, 7 Nov 1996 17:50:53 -0800 (PST)
(6) From: "M. Bottoms" <ambottomol67832.cc.nps.navy.mil>
(7) To: Tom Whitt <to whitt@$m.ir.lo.COM>
(8) Cc: Real 3D <real3d@mmc.com, Denise Adams <zzxxms@ldsa.com,
    Joe Arion <oerion@aol.com>, BALCERAK <LCERAK@AR'A.mll>
```

- **Line (1)** tells other computers who really sent the message, and where to send error messages (bounces and warnings).
- **Lines (2)** and **(3)** show the route the message took from sending to delivery.
  - Each computer that receives this message adds a Received: field with its complete address and time stamp; this helps in tracking delivery problems.
- **Line (4)** is the Message-ID, a unique identifier for this specific message. This ID is logged, and can be traced through computers on the message route if there is a need to track the mail.
- **Line (5)** shows the date, time, and time zone when the message was sent.
- **Line (6)** tells the name and e-mail address of the message originator (the "sender").
- **Line (7)** shows the name and e-mail address of the primary recipient; the address may be for a:
  - mailing list,
  - system-wide alias,
  - a personal username.
- **Line (8)** lists the names and e-mail addresses of the "courtesy copy" recipients of the message. There may be "Bcc:" recipients as well; these "blind carbon copy" recipients get copies of the message, but their namesand addresses are not visible in the headers.

Chairperson FEINSTEIN. Thanks very much.

We will begin the questions, and I am going to ask you one, Mr. Savage, if I may. The Secret Service does not participate in the NIPC, right?

Mr. SAVAGE. That is correct, Madam Chairman.

Chairperson FEINSTEIN. And why is that?

Mr. SAVAGE. We don't participate in a formal setting at this time. We have, I believe, a very good and improving relationship with the NIPC at this time. Just last week, I was on the phone probably at least a dozen times personally with personnel with the NIPC.

We collaborate on cases of interest. We are also participating with the NIPC and the FBI with respect to some of the e-commerce cases that were mentioned, and we are currently discussing the possibility for a future formalized return there.

Chairperson FEINSTEIN. All right, thank you.

Mr. Dick, you might be interested. My Judiciary counsel, Matt Lamberti, told Senator Kyl and I a story on our way to the vote that I want to relay to you. He said this past weekend that his girlfriend received an e-mail on her computer from her uncle and there was an attachment. And, while the e-mail didn't seem right, she opened the attachment and there was a lot of irrelevant stuff on it. She then got another e-mail from the uncle that said don't open any attachments; an attachment with a virus just ruined my hard drive. So Matt Lamberti keyed into your service and, through the Internet, downloaded software onto her computer which prevented the virus from being effective.

Mr. DICK. Thank you.

Chairperson FEINSTEIN. So that was an actual instance of progress.

I wanted to ask you this question as well: Terrorist groups are increasingly using computers and the Internet to develop plans, to raise money, to spread propaganda, as well as to communicate. Hizbollah, Hamas, the Abu Nidal organization, and the Bin Laden organization all rely on computers, e-mail and encryption to support their activities. There are even reports that a group affiliated with the Tamil Tigers has attacked foreign government Web sites.

What information can you share with us in this setting about cyber attacks by international terrorist organizations?

Mr. DICK. Madam Chairwoman, everything you just described is very accurate insofar as the threat is concerned. Obviously, this is a high priority within the Center, within the FBI and the other Government agencies that we deal with, is the threat that would come from terrorist activity.

We have been very fortunate insofar as we have not been able to identify any known terrorist organizations using cyber means to attack facilities here in the United States. Now, not for this environment but perhaps another one, we can talk about issues in other countries. But as I have said many times, the threat is real, the potential for its use is very high, in our belief, and we need to be very diligent with our partners to protect ourselves.

Chairperson FEINSTEIN. How many of the NIPC's closed cases involve threats or attacks on our Nation's critical infrastructures, and were these cases really a threat?

Mr. DICK. You mean critical infrastructures in those that would be defined as vital to our economic well-being and national security?

Chairperson FEINSTEIN. Yes.

Mr. DICK. I don't have those figures readily available to me. One of things you have to realize about the Internet, and I am sure you are well aware, is that whenever you have an intrusion, we conduct investigations, and we conduct investigations that use the law enforcement authorities that are available to us because we never know who is behind that keyboard until we arrive behind that keyboard. So every investigation that we open up, we look at it in the

context that it could be some 15-year-old criminal, but it also could be some sort of state-sponsored activity.

Chairperson FEINSTEIN. Yes. We have actually had the classified briefing on some of this. I would like to ask you, though, in writing, if you could give us a listing of those cases that you believe really are a threat or were a threat.

Do you happen to know, of the pending cases, how many involve threats or attacks to our critical infrastructures?

Mr. DICK. I would be just taking a wild guess.

Chairperson FEINSTEIN. Can you give me just a percentage?

Mr. DICK. Many of the cases obviously involve crimes for greed, but those that I would rank in national security concern are probably 10 percent.

Chairperson FEINSTEIN. Ten percent?

Mr. DICK. I think of the level that you are probably referring to.

Chairperson FEINSTEIN. And can you give me the number you have of pending cases?

Mr. DICK. Twelve hundred, but that is a guess.

Chairperson FEINSTEIN. So it is 10 percent of 1,200, OK.

Do you happen to have the GAO report in front of you?

Mr. DICK. Yes.

Chairperson FEINSTEIN. I would like to ask you in the Executive Summary to respond particularly to those recommendations that I mentioned earlier. Let's go to page 12, the three factors that the GAO points out have hindered your ability to develop strategic analytic capabilities: no generally accepted methodology for analyzing strategic cyber-based threats, prolonged leadership vacancies, and lack of adequate staff expertise. I understand you have picked up on some of this, but I would like you to comment. You have been operating with only 13 of the 24 analysts that officials estimate are needed to develop analytical capabilities. Could you give us a progress report on those three things?

Mr. DICK. Insofar as the GAO's report and its assessment of our strategic capabilities, I frankly am in concurrence with what they had said there. We do need improvement in that area. As was articulated in the report, part of the issues associated deal with the leadership of the Analysis and Warning Section which is primarily responsible for the production of that.

Since GAO did its report, we have had a number of changes in that regard. No. 1, sitting behind me is Admiral Plehal, who is a two-star admiral from the United States Navy who has been detailed as my deputy to the Center to help in this regard insofar as developing a process by which to provide more strategic information to our partners.

In addition, the CIA has named an SIS individual to head up the Analysis and Warning Section. He has been on duty, I think, approximately 2 months and is making great strides insofar as his assessment as to what we need to do to provide the kind of strategic analysis that we need to do in the future.

We have just gone through the process of meeting with NSA and doing interviews of individuals who will head up our Analysis and Information-Sharing Unit. We have actually selected an individual and made a recommendation to NSA for the reporting of that individual.

With the Department of Defense and our watch capabilities which is specifically designed for them in the Analysis and Warning Section, Admiral Plehal is working everyday trying to get a final commitment in that regard, which I believe we will. So I think that we are making great progress in that regard.

In addition to the leadership positions within the Department of Defense, for example, Admiral Plehal has been working with them insofar as filling of certain vacancies over there that we have. Currently, we have about 18 detailees on board and we fully expect to reach maximum capability in that in the very near future.

Chairperson FEINSTEIN. Is that the 18 out of 24?

Mr. DICK. We have always had a goal of 40. There has never been a chiseled-in-stone number, but the goal has always been 40. We have never reached it. We have hovered around 20, 22. I would have to look, but I think it is around 18 or 20 that are there now, but the point being that because of Admiral Plehal and the leadership from the CIA, we now have a plan in place by which to fill those positions.

Another point I would like to make is one of the things that we are trying to do from the Center is to have our partners believe that they own or have ownership in the Center. One of the things that we are doing is I have established regular meetings with seniors from the other agencies to discuss Center issues as to what kinds of products do they want to receive from us, what is it they expect from us to facilitate in the area defining what is the strategic analysis that you want to receive from us. Through that, they will discern how can they facilitate our efforts for the community at large to provide those products. So I have to be able to get them to feel they own the Center in some respect.

Do you want me to go through all of them?

Chairperson FEINSTEIN. I think we would like to know what progress has been made, wherever you can do it.

Mr. DICK. OK. Insofar as the issue concerning information and our abilities to data-mine and warehousing of data, we are in the process of completing that project. Obviously, data-warehousing and data-mining is going to be a multi-year-funded issue; it just doesn't stop because of the inflow of information.

But at this point in time, we are beginning to do data-mining and receiving of information from our field offices that are called 801s, where they report incident information. That piece of the data-mining project is in final phases of completion where information can be shared in that regard.

Insofar as the performance measures, we have sent our policy statements to our field offices to discern what kinds of information they are receiving insofar as computer intrusions are concerned, developed a statistical basis by which to claim those statistics so that we can track them, and I think that we are making progress in that regard.

Insofar as the ELES, or Emergency Law Enforcement Section plan, as I mentioned in my statement that has been completed. But, again, that is going to be an ongoing process with the Emergency Law Enforcement Sector Forum to continue to implement these recommendations that occur out of it.

Insofar as our formalized relationships with the ISACs, as I mentioned a moment ago and as mentioned earlier, we do have one formalized ISAC agreement with NERC. We are in the process of negotiating others, but just because we don't have a formalized process or MOU, if you will, with the financial services ISAC or the other two doesn't mean that we are not in the process of information-sharing, as I pointed out in the e-commerce vulnerabilities, where we work fairly routinely with alerts and advisories and get their counsel in that regard.

Insofar as information-sharing and exchange is concerned, we talked a little bit about that and I believe that in the not too distant future we will have agreements and understandings with each one of the ISACs. In fact, I have been talking very closely with Howard Schmidt, who is heading up the IT ISAC. Howard Schmidt is with Microsoft, and as soon as they formalize how they are going to operate there is a great willingness on their part to discern how we are going to share and receive information back and forth from them. We have those kinds of relationships with every one of the ISACs.

Did I miss any?

Chairperson FEINSTEIN. If you just go to the bottom of page 15, the recommendation that the FBI Director and the Attorney General ensure that you have access to computer and communications resources, monitor the implementation of new performance measures, and develop an emergency law enforcement plan. Has any of that taken place?

Mr. DICK. The plan, as I have said, is complete. We turned it into the National Security Council and the White House March 2 of this year, so that is completed.

Insofar as the resource requests, obviously we are going through the various budgetary processes, and the administration obviously prioritizes those requests, but we have made such a request through the administration.

As I mentioned a moment ago, we are monitoring the implementation of the new performance measures out there through our own field offices and getting reporting in that regard. But there is more that needs to be done.

Chairperson FEINSTEIN. One last question. It has come to our attention that President Bush is considering issuing an executive order reorganizing the administration's policy in combatting cyber crime. Some details have been in the press. What has been reported is that an advisory board with representatives from over 20 Federal agencies would coordinate administration efforts to combat cyber crime. The Chairman of that board would report to the National Security Adviser.

What would be the NIPC's role if this is an accurately reported executive order and when do you think that executive order will be forthcoming?

Mr. DICK. I as the Director of the Center have been involved with the administration, as well as heads of the other Government agencies, in the review of that executive order. I think it is the administration's intent in the creation of the board to raise the level within the public and private sector of information assurance such that information assurance is not just a collateral duty of the head of an

agency or a CEO, but a primary duty and a priority for that head of the agency.

Insofar as our involvement, in the last draft that I saw of the executive order the Director of the NIPC would actually be on the board and a participant on the board, and hopefully an active participant in that regard. So we are very supportive of what the administration is trying to do. Now, insofar as when the administration will issue it, it is out of my control.

Chairperson FEINSTEIN. Thanks very much, Mr. Dick and Mr. Savage.

Senator Kyl?

Senator KYL. Thank you, Madam Chairman. Let me first note that Jim Savage was a detailee in my office for almost a year from the Secret Service and did an excellent job. I am an advocate of detailees partially because of the efforts of people like Jim Savage.

I am a little concerned that we haven't helped to make it easier for detailees to be utilized better by NIPC. I understand one of the problems is a lack of reimbursement to the host agency or the gifting agency, or whatever you call it, and, second, that nobody has any expertise to spare. I ask any of you what we can do to help address that problem so that NIPC can get more high-quality detailees.

And the second part of my question is specifically to Mr. Dick. One of the criticisms in the report was the under-utilization of these detailees and I would like to have you respond to that.

Mr. DICK. I can go first, I guess. I can't speak for the past; I can certainly speak for since I have been director and the time I have been in the Center. You can call Admiral Plehal up, but I don't know of any resources, particularly technical expertise, that is under-utilized within the Center.

I have got people, as I have said in my written statement, that are very dedicated, hard-working people that are working 12, 14 hours a day, weekends, particularly of late with the Leaves as well as Code Red viruses. They are giving it 110, 120 percent.

I am not sure where that came from in the past, but I assure you that isn't the case today. Frankly, one of the things we have been talking about is burn-out, and I know all of our agencies are in the same boat. We are stretching our resources as thin as they can be and we are going to need to do something about it.

Senator KYL. How can we get good, expert detailees from these other departments?

Mr. DICK. That is a very good question. In my experience with the other agencies, it is not a matter of desire; it is a matter of having the ability to have someone fulfill the functions they are doing when they leave. Obviously, that is a resource and funding issue.

Senator KYL. It seems to me it is also a leadership issue, though. I can't think of anything more important than making this NIPC and the related aspects of it work properly. Each of the agencies involved have important functions, no question about it, but protecting the Nation against cyber crime and cyber terrorism and cyber attack has to rank right up there at the top. I mean, I don't know of anything more important than national security, for example.

So any of you who have any suggestion about what we can do to provide the leadership—I mean, do we have to have the President or the Vice President put out a notice and say, look, guys, I am going to be checking back, this is my priority, make somebody available? I mean, is that what it is going to take?

Ms. MCDONALD. Sir, if I may, the General Services Administration has had somebody at the NIPC since its inception to address the concern that was brought out by GAO that perhaps maybe some of the detailees were not tasked as well as they should. I know that in our case we had sent an individual over as a liaison, and partly it was an error on our part. We didn't have the individual actually working in one of the units; he was more working in a liaison capacity. He wasn't involved in the work. Since then, we have amended that work arrangement and it is working much better.

As far as additional resources for the NIPC, the entire Government has a very difficult situation because we cannot attract qualified people in this arena. So an agency that gets somebody who is qualified in the security arena is very reluctant to let that person go, so it is a larger issue than the NIPC. Reimbursement would assist, but that is not the entire answer.

Senator KYL. I am sure that is the case. Everybody we talk to needs qualified people. I had a question for Mr. Savage in this regard.

At least I am informed that the Secret Service has a very good program to train agents as computer investigative specialists. It has been very successful. If that is true, what suggestions would you have for other agencies to train the number of people that are needed here?

Mr. SAVAGE. Senator, I would like to thank you for your previous kind comments on my behalf and I would like to respond to your question. The Secret Service does have what we believe to be a very good program. As a matter of fact, we partner with other three Treasury agencies in that regard. We have trained approximately 50 agents this year in that respect.

We have actually been approached not only by State and local officers, whom we believe are an important part of this effort, but we have also been approached by other smaller Federal agencies as to how they might be able to start programs of a similar nature. What we have done is shared with them our past trials and tribulations and what has worked for us and what has not.

What we are seeing on other Federal agencies is exactly what we have seen, and that is the issue of cyber crime and computer forensics completely transcends all portions of the operations and other aspects of other agencies, even if they are not involved in the law enforcement effort. So what we have tried to do is impart that past knowledge that we have learned.

Senator KYL. So, within limits, you would be willing to help others if they come to you and need a little expertise in getting a training program underway?

Mr. SAVAGE. Absolutely, Senator. As a matter of fact, the private sector, as well, seeks our input and we are more than happy to accommodate. We feel as public servants that is part of what we can do.

Senator KYL. Well, maybe one of the things we need to address is what we can do on a broader scale to make sure that we have the personnel available here.

What is holding up the formal agreements with the other ISACs? Is there anything generic? This has been going on quite a long time now. What is taking so long? Is it just a matter of filling in some blanks here or is there some generic problem, especially one that we might help to address?

Mr. DICK. From my standpoint, I don't know that there is one specific issue or problem because information-sharing comes down to one simple word; it comes down to "trust." Trust is one of those things that is not legislated. You can't mandate it. It takes time and experience dealing with each other for that to evolve.

For example, with NERC, we have had a long history with the electrical power sector in working together from a physical infrastructure standpoint. There has been a lot of trust that has built up not only with us in Government, but with the other partners in the electrical power sector, because they have to share information and share the power grid, and so forth. So the trust was built-in in that area.

Financial services is a different arena. It is very competitive. I think what we are experiencing in this regard, in my opinion, is that through dealing with each other, through sharing information, through seeing that we can work together to the benefit of each other, more and more information is flowing. Through that trust building up, we will come to the resolution of agreements.

It doesn't mean that information isn't flowing because there is not an agreement there, because it is. The volume of the information that is flowing is the key, and that is dependent upon the trust over time.

Senator KYL. Well, are there specific problems that industry has raised? For example, from time to time we hear concerns expressed about the antitrust laws potentially presenting a problem of industry folks getting together to talk about certain things, the FOIA problem that I mentioned before about providing information that then could be subject to mandatory release.

I am also specifically interested, Mr. Dacey, in anything you picked up during the investigation that might help us determine whether there is something we can do to facilitate this trust.

Mr. DICK. We are absolutely supportive of legislation that would encourage the private sector to voluntarily provide the Government, not just the NIPC, but the Government with more critical infrastructure information. There has been concern, as you rightly pointed out, and the Chair and you, as well as Senator Bennett, have worked, I think, very hard in trying to clarify the Freedom of Information Act so that the private sector would be encouraged to provide this information. I think if that provides the assurances to the private sector and the safeguards that they seek, then we should pursue that.

Senator KYL. Mr. Dacey, any other comments?

Mr. DACEY. Basically, I have similar comments. I think anything that could be done to encourage the sharing of that information would be productive and those areas ought to be investigated for possible changes. I know you had the interest and Senator Bennett,

as well as the House last year had a bill that they were discussing in this area.

Senator KYL. Well, there are a couple of other questions I might submit to you for the record and I would like to ask you to take under advisement the last two questions, really the question about are there endemic problems here that we could help address with these agreements, and, second, are there any other ways that we can help to train personnel. Any thoughts you have in that regard, I would like to have you communicate them to us.

We have another panel, so I am going to just ask one final question, and that is the question about the NIPC's authority. Do you think that by now it is clear? Do you think it needs to be clarified, Mr. Dacey? And any particular comments, Mr. Dick, that you would have about the authority?

Mr. DACEY. When we did our review, we got some conflicting views about what the roles and responsibilities of NIPC were based on PDD–63, and we put in our report a discussion of that, ranging from the national coordinator to others.

I think it is important that that role be clarified so that everybody understands whose responsibility it is for critical infrastructure. We have already got a number of entities involved in critical infrastructure, many of which have been named today. So I think it is just important that that role be clarified.

In terms of clarification, we have heard that the discussions with this executive order and discussions with the new national plan may address some of those issues. At this point, though, we really haven't seen anything specific that addresses those issues.

Senator KYL. Well, I think Senator Feinstein mentioned that and perhaps we can also make an inquiry and ensure that if there is further work done in this regard by the administration that that is one of the things that it addresses.

There is much more to go into, Madam Chairman. I think what I will do is just submit a couple of questions for the panelists for the record and pass it back to you.

Chairperson FEINSTEIN. Thanks very much.

Both Senator Kyl and I are very concerned with combatting terrorism. We are also members of the Intelligence Committee. We are aware that our efforts in this area are spread over some 41 different departments.

I would like to ask you, Mr. Dick, to arrange for us another classified briefing on terrorist cyber threats. I can't remember when we had the last one. Was it 2 years ago? But I think we need to get updated on some of those groups that are known and operating in the area.

You mentioned Senator Kyl and Senator Bennett's legislation. How do you believe we can better handle the Freedom of Information Act issue with private companies, just straight exempting them from FOIA in this situation, or do you have other recommendations?

Mr. DICK. Again, based upon my experience before I came into this job with the financial sector, there were safe harbors when the suspicious activity reporting was developed many years ago in the banking and finance area which provided the banking and finance sectors some safe harbor regarding the protection of that informa-

tion and providing it. Perhaps that is a model that could be used, but there is greater expertise up on this Hill than I have in that regard.

All I know is we believe that we have sufficient authorities to protect it. The private sector is not comfortable with it and we need to do something to make them feel comfortable because it is not a matter of they don't want to provide it; they just don't feel comfortable providing it.

Chairperson FEINSTEIN. So you are saying create a safe harbor that if you report this kind of information, you are not subject to FOIA?

Mr. DICK. Right, because we believe we have that ability now, but some in the private sector do not.

Chairperson FEINSTEIN. Do you have any thoughts on whether the FBI would need an administrative subpoena power?

Mr. DICK. I have several thoughts on issues regarding the legislation, if you would care for me to talk about a couple of them.

Chairperson FEINSTEIN. Please.

Mr. DICK. One of them deals with Title 18 United States Code Section 1030. It defines that if an individual intrudes into a system and basically takes it over, we have to be able to demonstrate that there was at least $5,000 in damage done to that computer before there is a Federal crime. That sometimes is problematic to us, particularly in the early stages of an investigation when you have had somebody who has intruded into it.

We believe that that might be more appropriately considered in determining penalties insofar as the damage is concerned. For example, the virus that are spreading out there now that come into your system, look at your address book and then re-e-mail them—the damages associated with that to individual computers are probably not going to reach that threshold. However, the totality of the damage that is done across the network will be substantial.

One of the other issues that we think needs to be looked at is pen trap and trace under Title 18 United States Code Section 3122. The language used in that statute is probably—how do I phrase this—technologically outdated and needs to be looked at insofar as the Internet is concerned.

It would be also beneficial for the courts if they could issue a nationwide order. One of the things that we continually run into is that there are different hop sites across the United States, as well as the world, and every time we go into a different judicial jurisdiction we have to go in and get another order or another pen trap and trace, or whatever, and it takes time. And as you well know, on the Internet things don't happen in minutes; they happen in nanoseconds.

Fourth, I think a significant point is in a number of agencies there is a need to review Title III to determine whether it needs clarification, and a clarification, for example, in Title 18 United States Code 2517. We may need to clarify to allow for quick sharing—I say quick sharing—from law enforcement to the intelligence community of information obtained in a criminal case under Title III that turns out to demonstrate an actual or potential act against the U.S. by a foreign power or agent of a foreign power.

So there are some legislative issues that I think could be looked at.

Chairperson FEINSTEIN. If you would be willing to make some recommendations to us in writing, I would appreciate that very much.

Mr. DICK. OK.

Chairperson FEINSTEIN. Senator Cleland, you wish to speak on the second panel, is that correct?

Senator CLELAND. At your wish, Madam Chairman, I have a distinguished panelist to present.

Chairperson FEINSTEIN. For the second panel?

Senator CLELAND. Yes, ma'am.

Chairperson FEINSTEIN. That is correct.

I think we are finished, unless you have additional questions.

Senator KYL. No. That is fine.

Chairperson FEINSTEIN. Let me thank this panel very, very much. We appreciate it. Thank you.

The second panel, if you would come forward, is Mr. Michehl Gent, the President of the North American Electric Reliability Council, and Mr. Chris Klaus, founder and chief technological officer of Internet Security Systems.

We have a surprise introducer in the form of the distinguished Senator from Georgia, Senator Cleland, and we are delighted to welcome you to our Subcommittee.

STATEMENT OF HON. MAX CLELAND, A U.S. SENATOR FROM THE STATE OF GEORGIA

Senator CLELAND. Thank you, Madam Chairman. It is a pleasure today to be with you and this distinguished panel to discuss the important topic of computer security.

Hackers and cyber thieves are presenting an ever-growing threat to technology infrastructure as we know it. Recent experiences like the Melissa and I Love You computer viruses remind us how vulnerable we really are to the crippling attacks of an individual or group with access to the technology to disable individual computers or entire networks.

I am particularly pleased this afternoon to introduce Mr. Christopher Klaus, founder and chief technology officer of Internet Security Systems, Incorporated, in Atlanta. Mr. Klaus, a graduate of the Georgia Institute of Technology, will provide you with some valuable background information and recommendations regarding the computer security threat.

Chris Klaus is regarded as one of the world's foremost security experts. In 1991, he became interested in Government security while interning at the Department of Energy. Chris then began working on a ground-breaking technology that actively identified and fixed computer security weaknesses.

The next year, while attending Georgia Tech, Chris released his product for free on the Internet. He soon learned the error of his ways. He received thousands of requests for his invention and decided he should sell it, in the great tradition of Thomas Edison. In 1992, he formed Internet Security Systems and developed the company's first software program and flagship product, Internet Scanner.

He has been the topic of numerous stories and has been quoted in such publications as the Wall Street Journal, Forbes, and CNN. He continues to represent ISS as a spokesperson at technology events, and provides high-level security consultation to a number of government organizations and Fortune 500 companies throughout the United States and abroad.

He was honored in MIT's magazine, Innovation Technology Review, as one of the top 100 young innovators for 1999. In addition, he received the award for Ernst and Young's Entrepreneur of the Year in 1999 in the category of internet products and services. He was the youngest person on the 1999 Forbes 100 high-tech wealthiest list, and his recent $15 million gift to Georgia Tech made him the youngest philanthropist to give a donation of this amount.

We will see you after the meeting.

[Laughter.]

Senator CLELAND. Chris' company, Internet Security Systems, is the worldwide leader in security management software. Internet Security Systems employs nearly 1,500 employees in 20 countries focused exclusively on computer security. The company serves more than 8,000 customers, including 68 percent of the Fortune 500, 21 of the 25 largest U.S. commercial banks, the 10 largest telecommunications companies, numerous U.S. Government agencies, and other non-U.S. Governments. Former Senator Sam Nunn, my predecessor, currently sits on the board of ISS.

Madam Chairman and members of the committee, I am delighted to present Mr. Christopher Klaus.

Chairperson FEINSTEIN. Thank you very much, Senator Cleland.

Mr. Klaus, after that introduction, we expect you to solve all the problems, and also add some spice to the hearing, being so young as well.

[Laughter.]

Chairperson FEINSTEIN. So, Mr. Gent, if you don't mind, we will begin with Mr. Klaus.

Senator, thank you very much for coming by and introducing him.

Senator CLELAND. Thank you.

STATEMENT OF CHRIS KLAUS, FOUNDER AND CHIEF TECHNOLOGY OFFICER, INTERNET SECURITY SYSTEMS, ATLANTA, GEORGIA

Mr. KLAUS. Thank you, Senator Cleland, and thank you for the opportunity, Madam Chairwoman and Senator Kyl, for allowing me to present today. I am here representing Internet Security Systems, as well as the ITAA, to talk about the background of security threats.

Many of the companies who are out there who are fighting the threat rely on both our technology that we pioneered as well as our managed services, where we are providing service on behalf of the companies or Government agencies.

I have prepared a demonstration or anatomy of an attack, just a high-level attack. Really, it is going to be broken into——

Chairperson FEINSTEIN. Let me just thank you. It is very thoughtful of you to make it two-sided—most people do not do

that—so that the people who are attending the hearing can also see it. So thank you very much.

Mr. KLAUS. Thank you.

There is an attack happening right now called Code Red worm, and there was a little bit of a mention, but I thought it might be useful to describe in detail kind of how it works and what the effects are. I think right now Code Red is a good example of an effective worm that, with minor tweaking, could be a lot more dangerous in terms of what it is doing. But let me talk about some of the details here.

We will start with a denial of service attack. A lot of people in the security industry know denial of service attacks as a way to break down or stop a company from interacting with the Internet. The way it works is a lot of these computers are set up connected to the Internet and they are typically accessing it through some kind of pipe, what you would call bandwidth, through their Internet service provider.

What an attacker would do is flood the computers or flood that pump with a bunch of garbage data, and if the hacker's computer can generate enough traffic and his pipe is bigger than the pipe of the victim, they can over-flood it. It is kind of like a toilet system where you put too much toilet paper in there and it floods up and puts it out of commission. Well, that is what the attacker is doing here.

The thing about this is a single computer probably doesn't have enough pipe in terms of bandwidth or enough toilet paper to clog up a large company's network. So what the intruders have done is come up with another method they call distributed denial of service of attack, and the way it works is basically there are thousands of computers out there that are vulnerable at universities, companies, government agencies.

What the hacker would do is we have a data base we have been collecting of vulnerabilities. We have close to 10,000 different vulnerabilities that we have catalogued and classified, and basically they affect every more operating system, from Microsoft, to Sun, HP, IBM. What the attackers do is they break into all these systems and they implant what we call a zombie client. It is a program that sits on the system.

From there, what they can do is once they have compromised, say, 100 machines, they can have all those machines simultaneously trying to flood somebody's network. So even a huge company with a large bandwidth or a large pipe, even an attacker that was trying to flood them probably would be more of an annoyance. But when you have over 100 companies all with these zombie clients all over the Internet simultaneously in parallel with the aggregate effect of this flooding happening, it can pretty much take out any computer on the Internet. We saw that last year with Yahoo and eBay and those companies, and that was with, I think, small fire power at that time.

Well, there is now a new attack we call Code Red worm, and the way it works is very similar. The Code Red worm was released at the beginning of July and what it does is it compromises, just like an attacker would, a set of machines using a known vulnerability. It actually attacks IIS Web servers.

The difference between this and an attacker is that because it is a worm and it is automated, it is much faster at finding systems that are vulnerable. Once it finds a system that is vulnerable, it puts itself on that system as a host and then from there that machine is then being used to propagate itself, so it rapidly geometrically grows. Today, there are over 300 machines infected with this worm because they haven't been patched for various vulnerabilities.

What happened was there was some analysis done saying, OK, on July 20 it would flood whitehouse.gov. Fortunately, the attacker hard-coded the IP address of whitehouse. gov, so the White House staff was able to change the IP address so that when the flood did come, it was going to the wrong address. The scary thing is it is very easy within the program to change that to any IP address or pick multiple targets in the future.

What we believe is the worm is actually stopped right now and it is flooding. After 7 days, at the end of the end of the month, it will then begin propagating again and it will continue. What we are seeing today, though, is——

Chairperson FEINSTEIN. Is that automatic?

Mr. KLAUS. It is automatic. It is written into the software. It switches from propagation mode to flooding mode, back to propagation mode.

What we are starting to see is variations of this virus—well, it is not really a virus, it is a worm, in that most viruses rely on you getting an e-mail and you clicking on it and, oops, I ran the attachment. Well, what is dangerous about this is that it doesn't require a person to sit there and click on the file. If the machine is vulnerable, it is going to infect it and take it over.

Right now, the analysis looks like it is sleeping until the beginning of August and then it will start again. We have already seen where people have done analysis saying, hey, there are some flaws in this worm. And now there are updated versions of the worm as people are improving it to be more effective.

So, that is basically one of the major threats out there and it is very effective just because it has hit hundreds of companies. I think, on average, it has scanned every Web site out there at least 20 times already. I saw that CNN and the Pentagon and a bunch of other places were infected by this worm. I think ultimately we need to have a program for stopping these worms.

The good thing is, technology-wise, we can solve this. It is just more of a resource and priority of saying we need to put burglar alarms on these systems and we need to put a fixed vulnerability process in place. We knew about this issue long before this worm emerged. It is just a matter of putting in the right processes to fix those.

Chairperson FEINSTEIN. Can I just quickly ask you one question? Can you backtrack to get to the perpetrators?

Mr. KLAUS. It is difficult because, for example, even if you track it back to somebody, if the person is doing it outside the U.S. typically there are no laws against it. So it is very hard to enforce it.

The I Love You virus—a guy wrote it in the Philippines and got caught and was let go the next day because there were no laws against it. So because it is an international issue, most of the time

we recommend to our clients you just protect yourself and make sure you are not liable for getting infected with the Red worm or perpetrating the Red worm because you are infected. Maybe from there, somebody else could attack from your network because of that.

In most cases, you can track back pretty close to where it was coming from, but one of the other issues that is a trend—we were just at Defcon. We have an X Force research team, about 200 researchers, and they stay on top of all the threats. At the Defcon hacker conference, which is based in Las Vegas, there were about 5,000 hackers and one of the themes was wireless technology.

It used to be that you could track somebody back because they dialed in to their ISP or their Internet service provider and you could look up the caller I.D. information and find out whether they are dialing in and go back to their house. With wireless technology, it has no security, or very little security by most implementations.

We are starting to see that a lot of the hackers are moving to that because there is no logging. So when someone breaks into a network through wireless, from there they can use that to spring-board in to attack any network they want. And the issue is when you go back to the logs, there are no logs other than the host company that was used to spring-board. I think that is going to be a huge issue to track some of the attackers that are out there.

So this is at a high level, what we are seeing with some of the threats that are appearing. The good thing, like I said, is there are methods to actually reducing the risk, I think, through the burglar alarm systems. We asked recently 100 companies how many of them do a monitoring of their network on a 24-by–7 basis. It was 100 CIOs of a Fortune 1,000 group of companies, and 2 people raised their hands that they actually monitor. Most of them don't. We do it today in the physical world with ADT, monitoring people's houses, homes, and businesses. We haven't quite gotten there with cyber security.

I don't know if there are any other questions on the Code Red worm.

Chairperson FEINSTEIN. If you could conclude so that we can hear Mr. Gent, I know Senator Kyl has to leave shortly and I want him to have a chance to ask some questions.

Mr. KLAUS. In regard to the NIPC, just a couple of closing comments in regard to that. We have been working with them. They have been doing a good job within the resources they have. One of the suggestions for improvement is to explore ways to speed up the process of getting the information and releases out to the industry.

I think information-sharing is key in the security industry. When I started in this, nobody wanted to talk about the security issues. It is starting to evolve. Companies are still reluctant to share sensitive information. I think that is an area we need to foster. We are very supportive of Senator Bennett and Senator Kyl's bill in regard to the FOIA and helping companies feel more comfortable in sharing the information.

Most companies that we talk to would prefer not to tell anybody about their hacks. We get called in all the time where they have been broken into and they say it is cheaper to fire the person or

not deal with it than have it go on in the public and ruin the brand or stock price and all that. So we would recommend that.

Also, we are very positive on the ISACs. I think it is slow to change the culture and the mind set of a lot of these security professionals, but we are starting to see a lot of shift and change there. A few years ago, financial institutions and others of our customers were saying we don't want to share any of this information. Today, they are starting to say, you know what, let's get together and share best practices. That is actually a good thing we are seeing out in the industry.

So with that, I would like to conclude.

[The prepared statement of Mr. Klaus follows:]

STATEMENT OF CHRIS KLAUS, FOUNDER AND CHIEF TECHNOLOGY OFFICER, INTERNET SECURITY SYSTEMS, ATLANTA, GEORGIA

I. INTRODUCTION

I'm here today representing my company, Internet Security Systems, and also ITAA (the Information Technology Association of America) to provide you with some background information and recommendations regarding the computer security threat. Every day, Internet Security Systems stops criminal hackers and cyberthieves by addressing vulnerabilities in computers. These individuals use the Internet for business-to-business warfare, for international cyber-terrorism, or to cause havoc and mayhem in our technology infrastructure. Internet Security Systems is involved in every aspect of computer security, whether in making the security products or in managing them. We also monitor networks and systems around the clock (24 x 7 x 365) from the US, Japan, South America, and Europe in our Security Operations Centers. We search for attacks and misuse, identify and prioritize security risks, and generate reports explaining the security risks and what can be done to fix them. At the heart of our solution is our team of world-class security experts focused on uncovering and protecting against the latest threats. This team of 200 global specialists, dubbed the X-Force, understands exactly how to transform the complex technical challenges into an effective, practical, and affordable strategy. Because of all of these capabilities, companies and governments turn to us as their trusted computer security advisor.

ITAA represents over 500 corporate member companies in the U.S., companies that build IT solutions for customers in industry and government. ITAA is a national leadership organization in the InfoSec area.

Over the years, I have watched computer vulnerabilities increase dramatically. The Internet is so useful for the very reasons that it is so vulnerable. To give you an idea of what we are dealing with, I'd like to share an analogy. I'll compare a computer to a house. Every computer connected to the Internet has the equivalent of 65,536 doors and windows which need to be locked and monitored to make sure no one breaks in. Multiply 65,536 by every computer in every company or household and you begin to see the extent of the problem. Just as physical security companies like ADT monitor your physical doors and windows, computer security companies must lock and monitor the doors and windows of computers.

II. EXAMPLE OF DENIAL-OF-SERVICE ATTACK

A denial-of-service attack, or "DoS", is a specific type of attack on a network that is designed to bring the network to its knees. A DoS causes a network to have zero accessibility by flooding it with useless Internet traffic and requests. Many DoS attacks exploit limitations in the network. During a distributed DoS attack, a hacker actually takes over multiple computers with a "zombie" program and then, from a remote location, sets them to launch an attack all at once. This attack makes it nearly impossible to trace the hacker since the attacks appear to have come from the infected computers - which could be anywhere, such as universities, the Federal Government, businesses, or your home. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being created by hackers. Last week's well-publicized Code Red email worm is an example of how a new DoS attack can be launched.

Code Red was designed to launch a DoS attack that would effectively shut down the White House's Web site last Thursday evening. Code Red took advantage of sys-

tems running commonly used,software. Due to Code Red, more than 200,000 servers were infected to act as "zombies" that would wake up and flood the White House Web site with DoS traffic in order to force the site to shut down.

The White House was fortunate and acted in time—in cooperation with industry—to side-step this attack, but Code Red has forced network and system administrators to spend hours installing and testing a patch for the infected servers. And some servers may remain infected, setting the stage for possible future attacks.

III. NIPC Discussion

I'm here to represent industry's viewpoint on the General Accounting Office (GAO) report entitled "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities". As you know, this report examines NIPC (National Infrastructure Protection Center) and recommends how NIPC can improve its ability to combat cybercrime and cyberterrorism. Before getting to the details of my findings and recommendations, I would like to point out that NIPC has made great strides. Ron Dick has been an effective leader and should be commended for his efforts in a very complicated job.

The GAO report had three main themes: 1) NIPC's limited analysis and warning capabilities; 2) lack of interagency cooperation at NIPC; and 3) reluctance of private companies to share information about cyberattacks with NIPC.

The GAO found that NIPC's analysis and warning capabilities were limited. It is our experience that the NIPC has excellent sources of information from law enforcement and intelligence sources. While we understand that some information cannot be shared due to its sensitive or classified nature, the NIPC makes every effort to craft its information into meaningful warning messages suitable for distribution to the widest possible audience.

Industry needs information as quickly as possible. However, we understand that NIPC puts a premium on accuracy in its warning products because it speaks for the federal government. Having worked with NIPC on warning products, we have seen this first hand. While obviously not all information can be provided to the private sector, in our experience NIPC shares a broad array of information with the private sector so it can be pondered and analyzed.

Because both speed and accuracy are important, NIPC should explore ways to improve the warning process so that it can put out the most accurate warning products it can in the fastest possible time.

GAO also pointed out that the reluctance of private companies to share information about cyberattacks was an issue in the effectiveness of NIPC. We agree that NIPC would be more

effective if the private sector shared more information with it, but we have seen great strides in information sharing over the past couple of years. The private sector not only runs private communications facilities, but also runs most of the Government communications facilities. We think that the ISACs (Information Sharing and Analysis Centers) and other information sharing mechanisms are a good mechanism for this information sharing to take place. However, the ISACs and other information sharing mechanisms need time to further develop. We at ISS are very supportive of ISACs and are doing our part to make this initiative as effective as possible.

We also support GAO's praise of Infraguard. Infraguard is an effective initiative.Infraguard is able to effectively get information out to the business and academic communities horizontally.

IV. Information sharing is the key

All of the above themes involve more information sharing. We have discussed how the Federal Government could be better at sharing information. Companies also could be better at sharing However, sharing information about corporate security practices is inherently difficult. Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either competitors or Government agencies. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments.

Allowing the ISACs time to develop and grow is one way the Government can help private companies become more amenable to sharing information. The voluntary nature of ISACs or information sharing bodies is extremely important. Attempting to force this to happen would be a disaster. As I mentioned earlier in my testimony, speed is extremely important for security information to be most useful. Placing burdensome requirements on companies would cause information sharing to be a legal and time-consuming process.

To help encourage growth of the ISACs, it is important to support legislation that will strengthen information sharing legal protections that shield U.S. critical infrastructures from cyber and physical attacks and threats. Legislation that will clarify and strengthen existing Freedom of Information Act and anti-trust exemptions, or otherwise create new means to promote critical infrastructure protection and assurance, would be very helpful. This legislation would likely have a catalytic effect on the initiatives that are currently under way. It is absolutely vital that we work collectively to remove barriers to information sharing. A broad industry coalition has been working with Senator Bennett and Senator Kyl on legislation in the Senate, and with Congressman Davis and Congressman Moran in the House. On behalf of ITAA, I want to express industry support for these bills.

V. CONCLUSION

We are pleased that the Government is interested in taking computer security seriously. The United States Government spends billions of dollars buying weapons and gaining intelligence to protect our country from more conventional types of attack. Our computer systems must also be adequately protected, or our entire infrastructure could be compromised by one person with one computer. Even though the task is complicated, computer systems can be protected.

The Government has taken great strides in the past few years. However, much, much more is needed. As industry has considerable resources and expertise, a continued partnership with industry is crucial. In addition, computer security must be a priority, and leadership and coordination are necessary in the Government. International leadership is also required. Perhaps most importantly, funding for secure Government systems must be increased by a substantial amount, and outsourcing should be considered as a viable, cost-effective option. The Government often does well with the resources it has been given. However, computer security specialists are required to implement and coordinate many different security products and services to adequately secure a system. As computer security expertise is extremely rare, the cost of computer security specialists is astronomical. To help address the cost of computer security, educational efforts must be undertaken to train the personnel required.

Thank you for inviting me here today. I look forward to a continuing dialog on the computer security issue, and hope that, working together, we can adequately secure our country's assets and information.

Chairperson FEINSTEIN. Thanks very much, Mr. Klaus.

Mr. Gent, I apologize for mispronouncing your name. Please proceed.

STATEMENT OF MICHEHL R. GENT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL, WASHINGTON, D.C.

Mr. GENT. Thank you, Madam Chairman, and good afternoon, Senator Kyl. I am here representing the North American Electric Reliability Council, and I am going to take the chairman's advice and cut my oral testimony short. If you have a copy of what was submitted, I won't be following it.

I think it is obvious from the comments of previous witnesses that NERC, as we call it, has a very active role in this whole theater of protecting electric systems against major catastrophes. In fact, that is why NERC was formed. We are ourselves an ISAC. We didn't invent that name, but when you think about what we do, we do information security and we do assessment.

We actually are responsible for coordinating the activities of some 150 control areas across the United States and Canada, and I have to emphasize the Canada part because as far as electricity goes, it does not know these country boundaries that we draw on maps and we have governments controlling. Electricity flows from Canada to the United States, and vice versa.

I want to get right to the points. I read the letter coming down this morning on the train. I apologize for not being more direct in my written testimony and I would like to answer your questions.

I think that our relationship with the NIPC works, and it works very well. We may be only one of the four that cleared the GAO's test screen, but we did clear it. We see absolutely no evidence that they are lacking in what they call interagency cooperation.

Now, for the private sector, we don't see a lot of this interagency bickering, but there was a time when we did, when sabotage and terrorism were very big issues. I think you might recall back in the late 1980's we had study task forces, and I believe that then Vice President Bush headed up a team appointed by President Reagan to deal with the sabotage and terrorism issue.

NERC became very much involved there and we saw an awful lot of interagency bickering. So what we did and what we have done ever since is we have cast our lot with the FBI. So when some agency wants to get involved—DOD, DOE; DOE is involved in many things—we tell them that we answer first and foremost to the FBI. And we are so committed to that that we quite periodically insist that all the electric utilities go reestablish their relationship at the local level with the local FBI office. Then we try to get the national FBI office to tell their local jurisdictions to go out and establish that contact.

So what happens is whenever there is a physical terrorism attack, sabotage attack, the first people they contact are the FBI, and it is the same with cyber attacks. So it was quite natural for us to take what we had done in the physical area, add cyber to it, and incorporate it in all of our notification procedures. That is why this has worked very well for us.

We also see no evidence where their capabilities are limited. We have had several instances where we have received advisories, and those advisories have been sent on through our communications system and been received by the proper individuals.

Now, at the heart of all of this is the willingness of the electric industry to work with the Government. Some people say that this is because we were once all monopolies and it was quite easy to coordinate among monopolies. That may well be true. Today, that monopoly system is disappearing, however, and we are still able to coordinate.

We have been asked by the Government, for instance, to deal with the EMP threats and we have done that. I mentioned dealing with sabotage and terrorism. All of you are familiar with the Y2K brouhaha that we had here a couple of years ago. The Department of Energy asked us to act to spearhead that with the electric utility industry and we did, and we think successfully. Now, we think we can also successfully handle cyber attacks.

With that, I think you are probably more interested in asking me questions than hearing me rattle on about our credentials for doing this, so I will leave it to you for the questions.

Thank you.

[The prepared statement of Mr. Gent follows:]

STATEMENT OF MICHEHL R. GENT, PRESIDENT, AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

THE ELECTRICITY SECTOR RESPONSE TO THE CRITICAL INFRASTRUCTURE PROTECTION CHALLENGE

My name is Michehl R. Gent, and I am President and Chief Executive Officer of the North American Electric Reliability Council (NERC). I am responsible for directing NERC's activities within the industry and with the federal government as these activities relate to terrorism and sabotage of the electric systems of North America. Since mid-1998, these activities include critical infrastructure protection.

NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. It works with all segments of the electric industry—investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; and power marketers—as well as customers to "keep the lights on" by developing and encouraging compliance with rules for the reliable operation of these systems. NERC comprises ten Regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

In my testimony I will discuss NERC's relationship with the National Infrastructure Protection Center and several related critical infrastructure protection programs that NERC participates in: Critical Infrastructure Protection Working Group; Indications, Analysis, and Warnings Program; Electricity Sector Information Sharing and Analysis Center; Critical Infrastructure Protection Planning; and Partnership for Critical Infrastructure Security.

SUMMARY

NERC has an excellent working relationship with the National Infrastructure Protection Center (NIPC). NERC and the electric industry worked closely with NIPC for about two years to develop a voluntary, industry-wide physical and cyber security indications, analysis, and warning (IAW) reporting procedure. This program provides NIPC with information that when combined with other intelligence available to it will allow NIPC to provide the electric industry with timely, accurate, and actionable alerts and warnings of imminent or emerging physical or cyber attacks. A high degree of cooperation with NIPC is possible because the industry has a long history of working with local, state, and federal government agencies. In addition, the NERC Board of Trustees in the late 1980s resolved that each electric utility should develop a close working relationship with its local Federal Bureau of Investigation (FBI) office, if it did not already have such a relationship. The Board also said the NERC staff should establish and maintain a working relationship with the FBI at the national level.

The Indications, Analysis, and Warnings Program (IAW) reporting procedure is modeled on an existing electric system disturbance reporting procedure in which electric utilities report system disturbances meeting predefined criteria to the U.S. Department of Energy. A pilot IAW program was field tested in one NERC Regional Reliability Council in the fall of 1999 and winter 1999/2000. The program was refined and rolled out to the industry via three workshops held during the fall of 2000 and winter 2000/2001. A comprehensive communications program is being developed to bring this program to the attention of those industry entities that were not able to participate in the workshops.

NERC NATIONAL INFRASTRUCTURE SECURITY ACTIVITIES

NERC has served on a number of occasions during the past decade as the electric utility industry (electricity sector) primary point of contact for issues relating to national security. Since the early 1980s, NERC has been involved with the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Year 2000 rollover impacts, and now the threat of cyber terrorism. At the heart of NERC's efforts has been a commitment to work with various federal government agencies such as the U.S. National Security Council, U.S. Department of Energy (DOE), and FBI to reduce the vulnerability of interconnected electric systems to such threats.

The report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to a May 1998 Presidential Decision Directive (PDD–63). PDD–63 called for government agencies to become involved in the process of developing a National Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the

country's critical systems through public-private partnerships. The PCCIP specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. In September 1998, Secretary of Energy Bill Richardson wrote to NERC Chairman Erle Nye seeking NERC's assistance, on behalf of the electricity sector, in developing a program for protecting the nation's critical electricity sector infrastructure. Responding to the (DOE) critical infrastructure protection initiative, NERC agreed to participate as the electricity sector coordinator.

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison, worked through its Infrastructure Assurance Outreach Program to perform an information assurance assessment for a small number of nodes on NERC's industry information system. The purpose of this assessment was to help NERC and the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. A second followon information system assessment was begun in late 2000 and will be completed shortly. The product of this study will be recommendations that will form the basis of a draft NERC policy on information assurance. In addition, to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America, DOE has provided clearances for a number of industry personnel and clearances for other key industry personnel are anticipated. These clearances compliment those obtained from the Federal Bureau of Investigation (FBI) as a result of encouragement by NIPC, as discussed below.

CRITICAL INFRASTRUCTURE PROTECTION WORKING GROUP

After several exploratory scoping sessions with DOE and NIPC, NERC created a Critical Infrastructure Protection (CIP) Forum to evaluate sharing cyber and physical incident data affecting the bulk electric systems in North America. The meetings of this group were widely noticed and the participants included all segments of the electric utility industry and representatives from several government agencies including the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, DOE, and NIPC. As a result of the groups' deliberations, NERC created a permanent group within the NERC committee structure—the Critical Infrastructure Protection Working Group (CIPWG). This working group reports to NERC's Operating Committee. It has Regional Reliability Council and industry sector representation as well as participation by the CIAO in the Department of Commerce, DOE, and NIPC.

INDICATIONS, ANALYSIS, AND WARNINGS PROGRAM

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

The electric industry Indications, Analysis, and Warnings Program, which evolved from this work (Attachment A), was presented to the NERC Operating Committee in July 2000 for discussion and approval. The Operating Committee approved a motion to implement the program; initial emphasis is on reporting by security coordinators and control areas. Individual electric utilities, marketers, and other electricity supply and delivery entities are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings and related materials. Workshops were conducted during the fall 2000 and winter 2001 to provide program details to the industry. A more comprehensive communications program is being developed by CIPWG to encourage broader industry participation in the program. NERC views the Indications, Analysis, and Warnings Program as a voluntary first step toward preparing the electricity sector to meet PDD–63 objectives.

ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS CENTER

The PCCIP recommended that each of the critical sectors establish an Information Sharing and Analysis Center (ISAC) to help protect the infrastructures from disrup-

tion arising from coordinated intrusion or attack. The ISACs would gather incident data from within their respective sectors, perform analyses to determine potential malicious intent, share findings with other ISACs (private and government) in a manner that assures, as required, target identity protection, and disseminate actionable warnings so appropriate action can be taken within each sector. ISACs would serve as points of contact between sectors to facilitate communications, especially during a time of stress. ISACs would study cross sector interdependencies to better understand and be prepared for the possible impacts of an "outage" of one sector on another.

The CIPWG has endorsed, and NERC has accepted, the naming of NERC as the Electricity Sector Information Sharing and Analysis Center (ES–ISAC). The functions performed are essentially the same as those functions that have been required of NERC for physical sabotage and terrorism. The ESISAC's duties are:

1. Receive voluntarily supplied incident data from electric industry entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.
3. Assist the NIPC personnel during its analyses on a cross private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts and other related materials to all those within the electric industry who wish to participate.

The ES–ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will likely request support for a 24-hour, seven days a week staffed facility. To this end, NERC also is exploring the feasibility of forming a joint ISAC with other sectors. NERC has established relationships with the other existing ISACs through the Partnership for Critical Infrastructure Security (see below) and will establish relationships with other ISACs as they form.

CRITICAL INFRASTRUCTURE PROTECTION PLANNING

The CIPWG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the electric industry (Attachment B). Separate business cases have been prepared for Chief Executive Officers, Chief Operating Officers, and a NERC general overview (Attachments C, D, E, and F). The purpose of the business case is to persuade industry participants of the need to report cyber intrusion incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPWG has developed a basic and fairly comprehensive plan to address CIP. The working group was concerned about generating an overly prescriptive plan too early in the process and has proceeded with a format that can assist in developing each entity's own plan. The prototype plan, which still is undergoing industry review, addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, reconstitution, and interdependencies between and among sectors.

The essence of this "Approach to Action" is being considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government. Richaard Clarke, Special Assistant to the President and National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, has discussed the importance of establishing and maintaining a National Plan to the health of the government and private sectors, companies, and the nation. Version 1.0 of the Plan did a good job covering the threats and the government response, but it did not detail private sector response.

The need for private sector participation is engendered by the fact that the government lacks private sector expertise and needs private sector "buy in" to CIP initiatives. The National Plan version 2.0, which will include private sector input, is scheduled for fall 2001.

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

The Partnership for Critical Infrastructure Security (PCIS) was proposed in late 1999 by members of several private sectors; the PCIS is supported by CIAO and the U.S. Chamber of Commerce. Earlier this year, it established itself as a not-for-profit organization and elected a Board of Directors and company officers. NERC participates in PCIS and I serve as its Secretary.

The PCIS Mission:

Coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

The PCIS held two general forums in 2000 and one so far this year. It is planning a second general forum on September 6–7, 2001. The PCIS has formed six active working groups: Interdependency Vulnerability Assessment and Risk Management; Information Sharing, Outreach and Awareness; Public Policy and Legislation; Research and Development and Workforce Development; Organization Issues and Public-Private Relations; and National Plan. The opportunities presented by PCIS include gaining a better perspective of the sector interdependencies, facilitating ISAC formation, and sharing of common research and development efforts.

EMERGING BUSINESS RISKS TO THE ELECTRIC POWER INFRASTRUCTURE

A CASE FOR CHIEF EXECUTIVE OFFICER ACTION

The introduction of competition in the wholesale and retail electricity markets, coupled with an increased demand for electricity, has led to electric utilities' to rely more on information technologies (IT). In addition to ensuring a utility's ability to generate, transmit, and distribute electricity to its customers, information systems are increasingly effective vehicles for exploring new markets; executing strategic business decisions; achieving internal operating efficiencies; and tracking the people, products, and services on which a firm's success depends.

The reliability and security of these systems are critical to electric utility survival. Chief Executive Officers (CEO), boards of directors, and other senior-level executives responsible for overseeing the business operations of electric utilities need to understand the risks posed by this increased reliance on information technology. In addition, they also must manage and, where possible, mitigate these risks to their organizations and the industry through continuous communication and leadership. This management and mitigation responsibility requires close coordination with finance, customer services, operations, and other senior-level officials in their firms, and coordination within the industry, to address a widening range of competitive and operational vulnerabilities, including information systems, security, and other cyber-related threats. CEOs, boards of directors, and other senior-level officials are vested with authority and have an obligation to manage risks and liabilities through due diligence and prudent management. As such, it is important that they recognize that IT is not only an enabler of competitive advantage, customer service, and investor confidence, but also a source of vulnerability or business risk.

What Is Changing?

Manned Facilities Operations	Unmanned Facilities .
Remote Monitoring	Automated Monitoring/Control .
Local Markets	Open, Reional/National Markets .
Local Customer Services	Consolidated Call Centers .
Customer Billing Information	Customer Services Information .
Heterogeneous Technology	Standardized/Homogeneous .
Traditional Electric Services	On-Line Businesses/E-Commerce .

BUSINESS OPERATIONAL SURVIVABILITY

Significant security risks stem from the interconnectedness of the communications networks that underpin utility generation, transmission, and distribution systems. Most of the approximately 3,200 electric utilities serving North America depend on IT networks, such as supervisory control and data acquisition (SCADA) systems, to manage generation, transmission, and distribution systems. These systems are linked to control networks and corporate management systems, many of which also are connected to systems outside the utility. In addition, the electric utilities participate in open markets, vastly expanding the size and complexity of the electric industry's IT infrastructure. Simply put, the electric industry, conducting arbitrage over real and virtual assets, relies on a nationwide network information systems to do business. These systems include Internet-based applications such as the Open Access Same-time Information System (OASIS), which facilitates the exchange of transmission availability information and on-line price negotiations.

Like commodities trading, the buying and selling of electricity would be virtually impossible without the efficiencies of IT. The array of mainframes, desktop clients, operating systems, and network protocols used by power marketers add to the complexity of the electric power industry's IT infrastructure. Consequently, as the newly competitive energy market matures, generation, transmission, and distribution systems will become increasingly subject to both IT- and market-related forces. This

maturation will present new challenges to ensuring the reliability of the electricity delivery systems in North America.

BUSINESS COMPETITIVENESS

Reliability and security have also come under pressure from financial interests. A utility's previous "obligation to serve" to some degree is being pressured by industry stakeholders. Many expect that a competitive market place will shift reliability from a mandated "obligation" to being a competitive feature of service in order to be in the electric business.[1] Many also see that the electric industry will become a highly competitive commodities business that is largely customer-driven and dependent on technological and operational efficiency. The Power Company of America expects annual trading volume of electricity to reach an unprecedented high of $2.5 trillion by the year 2003.[2]

If this projection holds true, electricity will become the United States' most heavily traded commodity. Consequently, power marketers and utilities are competing aggressively for a substantial share of the market. Like the financial industry's commodities market, which may be a harbinger of how the electricity market will evolve, electricity worth billions of dollars will be traded over computer-controlled networks and telecommunications systems. Failure to maintain the confidentiality, integrity, and availability of these transactions could not only compromise an electric utility's business strategy but, if widespread, could also threaten the confidence of those participating in the electricity markets.

Chairperson FEINSTEIN. Thank you very much.

Mr. Klaus, if I may, at least 4 days before the February 2000 distributed denial of service attacks, computer experts at some of the Nation's largest banks received detailed warnings of possible attacks from the banking industry's warning network. These warnings helped the banks protect themselves, as you mentioned, from the attacks that shut down Yahoo, eBay and other companies.

However, under Treasury Department restrictions, these warnings were not turned over to anyone outside the financial services industry, including law enforcement, so companies in other industries did not benefit.

Do you think the ISAC model is the most effective way of protecting companies from cyberattacks, and how do we better encourage information-sharing between industries?

Mr. KLAUS. I think the ISACs lay the foundation for sharing the information. I think with the distributed denial of service attacks, the biggest issue I see with the security is just from a priority perspective. It is usually an after-thought when people are designing their networks and they are implementing their computer systems. The information is out there.

In many cases like this worm, we knew about the IIS Web server vulnerability at least a month before the worm ever spread, but there were still 300,000 Web servers that were vulnerable. I guess the question will be how do we get people to put the resources in there.

One of the aspects that we are seeing is insurance companies are becoming a driver for this, where they are selling hacker insurance or cyber security insurance, where they are saying we are not going to insure you unless you have a standard level of security. That is having an effect. Before, we could easily over the Internet grab the whole data base of credit cards.

---

[1] John D. Mountford and Ricardo R. Austria, "Keeping the Lights On!" IEEE Spectrum (June 1999): 34.

[2] Tami Cissna, "Wholesale Electric Power Sales Are Increasing-Is Anyone Profiting?" Electric Light & Power (August 1998): 42.

That is one of the misperceptions, is with the credit cards, encryption fixes that, when, in fact, most of the attacks that we are finding—we are working with a lot of banks right now where it is not when you are Web-surfing and you put in your credit card. Most people ask, should I do that, and the answer is it is probably encrypted.

Where the attack is happening is the hackers go right into the data base itself, like the Oracle data base, and you can use the user name "Oracle" and the password "Oracle." Any of the data bases have default accounts that never get changed, so you can grab every credit card that exists on that data base. So having some kind of standard level of security for most of those systems would help, I guess, raise the bar for most of the intruders.

Information-sharing is good, but I would still say that a lot of that information exists today you can get out there. And ISACs help foster that, but I think the next thing will be how do we motivate industries to protect against those, once you have the information.

Chairperson FEINSTEIN. Mr. Gent, would you respond to that, and would you also respond to what the possibilities are of an attack on California's electricity grid, how likely it is and how it can be prevented.

Mr. GENT. Right here on national TV?

Chairperson FEINSTEIN. Well, we can arrange that it not be done on national TV, if you would like.

Mr. GENT. I think you are probably familiar with that one incident that happened to a Web server, the Cal ISO. The reporting was grossly overblown, and I was very happy to see that happen, actually. If hackers are going to attack Web sites that are holding information sources and not control sites, then I am perfectly happy with that.

Electric systems are controlled by computers we call EMS systems, energy management systems, and for the most part they are not vulnerable to the same type of hacker attack, with one exception, and Chris pointed it out. The vendors very often will have default ways into the system so they can pull maintenance.

Chairperson FEINSTEIN. And not a worm either?

Mr. GENT. No, but it could be, but it is not in this case. I believe you have to have a program running to be able to host a worm.

What we have tried to do is to make this whole problem a business problem, and part of the stuff that I turned in with my testimony are brochures that we have produced with the help of the CIAO, "Business Case for Action: A Case for Chief Executive Officer Action," what can an electric utility's chief information officer do, what utility operations executive do and what can NERC do?

As Chris has stated, we have got to get them interested in doing this.

One of the reasons that we have been so successful with large catastrophes like sabotage, terrorism, and so on, is that if you take out a very large facility, it will affect every utility on the network. In this case, if you attack a particular utility's Web site, the chances are you are only affecting that one business and you are not affecting companion businesses down the chain. So it is difficult

to get them involved and interested, but that is what we are trying to do here, with the help of NIPC.

To answer your question directly, I think there is little chance that the hackers can do any harm to either California or anything else in the West as far as operational control.

Chairperson FEINSTEIN. Little chance, you say?

Mr. GENT. Little chance.

Chairperson FEINSTEIN. Little chance. That is good news.

Mr. GENT. I hate to say never. I would like to, but I am not going to.

Chairperson FEINSTEIN. Thank you.

Senator Kyl?

Senator KYL. Thank you, Madam Chairman. I just would note that we had an example in Arizona testified to by our State attorney general that a hacker wanting to erase his electric bill essentially got into the electric utility——

Chairperson FEINSTEIN. You are on national TV, Senator.

Senator KYL.—got into the utility that had his accounts. That utility also, however, is responsible for all of the dams that contain the water that provide the water source for the Phoenix metropolitan area. Once he was in, there would have been nothing to stop him from automatically opening the dams and letting all the water out, which would have created a huge problem. It simply illustrates the fact that it is possible to break in, and somebody who could break in for one purpose perhaps even inadvertently could cause some other kinds of problems. So it is not a trivial issue in any event.

I have been asked to say that Senator Hatch intended to be here to participate in the hearing today. I know he has been detained and I would like to ask unanimous consent that his statement be submitted for the record, Madam Chairman.

Chairperson FEINSTEIN. So ordered.

[The prepared statement of Senator Hatch follows:]

STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

IMPROVING OUR ABILITY TO FIGHT CYBER-CRIME:

OVERSIGHT OF THE NATIONAL INFRASTRUCTURE PROTECTION CENTER

There was a time when a battle began with the sound of a trumpet and a cavalry charge.

In the 20th century, a battle was likely to begin with the sound of airplane engines on a bombing run.

In this new century, a battle will likely begin with the sound of a person typing at a computer keyboard, and the release of an electronic virus designed to paralyze an adversary's computers.

And it is not only warfare that is changing.

No longer do aspiring bank robbers need to don a ski-mask and carry a shotgun into a bank. Millions of dollars can be stolen electronically by illegally accessing the computer networks of the financial services industry.

No longer do aspiring terrorists need to plant a bomb to draw attention to their cause. Millions of people's lives can be threatened electronically—by disrupting air traffic control functions; or shutting down a power grid; or blocking access to 911 operators.

As a recently as a decade ago, these threats were barely imagined. And it is only in the last three years that the federal government has formulated a comprehensive strategy to protect the nation's basic computer infrastructure from malicious attacks made by criminals, terrorists, and hostile foreign states.

The National Infrastructure Protection Center has, for the last three years, been on the forefront of protecting our country's computer networks from outside attack. And, given where we were just three years ago, the NIPC has laid an important foundation in the protection of our critical computer infrastructure.

But the integrity of our computer infrastructure is so vital to our well-being as a nation, and the technology is evolving at such a rapid rate, that it is essential that we continue to reevaluate whether the federal government is doing everything it can do to protect our critical computer infrastructure. And for that reason, I applaud Senator Feinstein, Senator Kyl, and the Senators on this subcommittee, not only for holding this hearing today, but also for having had the foresight, over a year ago, to order the GAO study that is the focus of today's hearing. As a result of that foresight, and the hard work of the GAO personnel who prepared the report, we are able to pursue today's inquiry at a much deeper level, and with a greater degree of insight, than would otherwise be possible. So I commend the senators on this subcommittee, and the hardworking staff at the GAO.

I have examined the GAO's report, and I find it to be, on the whole, a balanced and wellreasoned assessment of the NIPC's performance. It highlights both the successes of the NIPC, and those areas where the NIPC has come up short of its original goals.

Not surprisingly, the NIPC has succeeded at those functions that are most traditionally within the expertise of the FBI, and it has been less successful at those functions that are least familiar to the Bureau.

The GAO found that "the NIPC has provided valuable support and coordination" in the investigation of computer crime. I agree, and I believe that the NIPC should be commended for its success, in a relatively short span of time, at making itself into a valuable resource for use by the law enforcement community when dealing with computer crime.

To facilitate the investigation of illegal access to computer networks, the NIPC has established teams of specially-trained computer crime investigators in each of the FBI's 56 field offices. In addition, the NIPC provides technical assistance to the field offices and coordinates investigations among the field offices. Since 1998, the NIPC has issued 93 warnings to systems administrators, alerting them, and the general public, about specific threats and vulnerabilities within their computer networks. An advisory issued in March of this year regarding a specific ecommerce vulnerability is estimated to have stopped over 1600 attempted hacking incidents.

Our experience over the last three years has shown the value of having a multiagency entity, like NIPC, with the resources to investigate computer intrusions that are often national in scope.

Obviously, there is room for improvement. The GAO report makes some specific recommendations to the NIPC leadership, such as improved information sharing between the NIPC and the agents in the field offices. I hope that the NIPC leadership gives serious consideration to these recommendations.

Some of the other problems identified in the GAO report appear to be beyond the control of the NIPC's leadership—such as the failure of agencies outside the FBI to provide full cooperation with the NIPC. We, in the Congress, must continue to exercise our oversight authority over the Executive Branch to ensure that all agencies are motivated to provide the needed cooperation in this vital area. I, for one, promise to do everything in my power to discourage institutional rivalries between the Executive Branch agencies from disrupting the important mission of the NIPC.

It is those functions furthest from the FBI's traditional responsibilities that the NIPC has had the most difficulty accomplishing. According to the GAO's findings, the NIPC has made little progress in producing a comprehensive, strategic analysis of the vulnerabilities of, and threats to, the nation's critical computer infrastructure. Similarly, the NIPC has not been particularly successful in establishing information-sharing arrangements with private industry.

The development of a comprehensive, strategic threat analysis is certainly one of the most important tasks that has been assigned to the NIPC. In the absence of such a strategic assessment, law enforcement will be perpetually consigned to responding reactively—instead of proactively addressing and eliminating threats to the system.

The GAO has identified several obstacles faced by the NIPC in performing its strategic assessment: the lack of an accepted methodology for evaluating threats; confusion within the Executive Branch about the scope of the NIPC's mandate; and inadequate technical expertise within the NIPC personnel.

Implicitly, the GAO report raises a fair question—that is, whether the NIPC, which has so far served principally as an "operational" organization, is the best entity within the federal government to conduct what appears to be an abstract, almost

academic, assessment of the strategic threats facing the critical computer infrastructure.

By giving voice to this question, I do not mean to suggest that I have reached an answer. I simply do not know, at this point, whether or not the NIPC is the ideal entity to perform this analysis. It may well be that the NIPC brings more technical expertise to this question than any other governmental entity.

The Administration has recently announced its intention to review Presidential Decision Directive 63, and to reevaluate the effectiveness of our national plan for cyberspace security and critical infrastructure protection. I hope and expect that, as part of this evaluation, the Administration will assess whether the NIPC is, in fact, the best entity to perform the strategic threat assessment. Certainly, I believe that Congress should await the Administration's determination on this matter, before reaching its own decision.

The other area which the GAO highlighted as a shortcoming in the NIPC's performance is the NIPC's lack of success in establishing information-sharing arrangements with private industry. It is in this area that I believe Congress could potentially provide the NIPC with the most help.

Obviously, the NIPC is hamstrung in its efforts to investigate computer intrusions when the private sector does not provide them with notification that an intrusion has occurred. On the other hand, private firms are often reluctant to report an intrusion, out of fear that publicity regarding an unauthorized intrusion will be detrimental to the firm's commercial interests. Although the NIPC has undertaken significant outreach efforts in an effort to win the private sector's confidence, there is little that the NIPC can do to overcome this basic divergence of interests.

It is possible, though, that Congress can help.

There is legislation pending, which I support, that would strengthen the FOIA exemption applicable to information provided by companies when they self-report an unauthorized computer intrusion.

I believe that Congress can go even farther. I believe that we should explore a range of financial incentives to the private sector—possibly tax credits or liability caps—for companies that provide the NIPC with full and timely notification of unauthorized computer intrusions. Only by reversing the private sector's financial incentives pertaining to cooperation with the NIPC can we enlist the aid of the private sector against the criminals and terrorists who would compromise our computer networks.

In sum, I believe we should commend the leadership of the NIPC, who have, in the short span of three years, laid the groundwork for a comprehensive defense of our critical computer infrastructure. As with any new venture, there have been successes, and there have been areas in which the leadership has fallen short of their goals.

Given the interconnected nature of today's digital world, it is impossible to overstate the importance of the NIPC's mission. Hopefully, the GAO Report, and today's hearing, have set in motion a healthy dialogue on how best to face these new and emerging threats to our well-being as a nation.

Senator KYL. I am going to have to go here in just a minute, but I guess one of the things that I should ask, since we have Chris Klaus' expertise here, is what are the first couple of things that you tell clients—I realize you have different kinds of clients come to you, whether it be a government client or a business client—when they say, well, what is the first thing I should do to protect myself or our company or our agency here?

It might be useful to at least give folks an idea of the kinds of advice that you give, and then I have one follow-up question, if I might.

Mr. KLAUS. We get a lot of companies coming to us saying, OK, I have heard security is important, what do we do? "Security" is such a big word. You hear about PKI, encryption, biometrics, firewalls, and the list goes on and on of all the different measures you can take.

Initially, what we do is start with an assessment in terms of doing an assessment of what your current state of security looks like. There are any number of security companies such as ourselves and many others that do assessments on behalf of companies.

It is kind of interesting, in that we are starting to see a trend where it is similar to the reason that you bring in the Big Five, like Ernst and Young or some of the other Big Five to do the books or the tax audits. It is the same reason you probably want a security team outside of that company to do a security audit to make sure it has not been tampered with.

It is very easy to configure the software to come back and say, OK, there are no problems, this must be a good network, so having someone come in, do a penetration test, find out all the issues, and then from there start to design your security system so that you can understand where to put the proper security processes in place.

I look at it a lot like physical security, in that there are certain places you may put a camera; there are certain places you will put locks, there are certain places you put guards, et cetera. The same metaphors can apply to a company's network. Where do you want a lock-down? What systems are critical? Where are your assets? Where are your key servers? What things do you want to lock down?

So we help design and then help deploy that, and then on an ongoing basis a high recommendation is to have a 24-by–7 monitoring and management of your security system. Security doesn't go away once you put it on the network; it is constantly there, and so we would recommend that.

And then the last thing would be education, get educated about all the different issues, know about what is a worm, what is a virus, how do you defend against those, what are the latest methods of breaking in. I think education and information becomes key there.

Senator KYL. It is just like security in any other setting, be aware of the potential dangers, get good people to give you advice about how to take care of it and then take care of it.

Mr. KLAUS. Absolutely.

Senator KYL. If you could give us some advice here, you are looking at this from two or three different angles. It is obviously useful for there to be an entity like NIPC to give warnings, to assist in remediation of problems, to have organizations like the one Mr. Gent represents to be coordinating very carefully with groups like NIPC.

You have seen the problems from the standpoint of both the private sector and the government clients that you represent. If you had to give us one or two suggestions about things that you think we might do to help to facilitate the exchange of information, to help entities like the one Mr. Gent represents, to improve NIPC, any of these things that we might do to help, what would be maybe the top one or two suggestions you could give to us?

Mr. KLAUS. Continue to raise cyber security as a high priority, and I think anything that can help raise the visibility and make sure people understand it is a serious issue that affects everyone. Also, I would say that one of the key issues we see—and this came from one of the industry analysts; they did a survey of companies and most companies spend more money on coffee and soda than they do on network security.

So from a budget perspective, I think both for commercial and government, if we can somehow give governments more money to

defend themselves so that they can hire the right people or at least get the right technology protection in place would be an additional benefit.

I think legislatively any of the bills that would help foster more sharing of information, and probably more than just fostering information, but trust and building a process for commercial to work with government—we had a large user base and there was a group of about 200 people of very large companies. How many of you ever worked with law enforcement in regard to being hacked? I mean, all of them had been hacked at some point, and one of them raised their hand and that person happened to be from a Government agency themselves and by Federal law had to do that. But the rest of them had not worked with any kind of law enforcement.

Chairperson FEINSTEIN. Would you allow me on that point——

Senator KYL. I am going to have to go. Might I just thank both of you and the other panel for being here, and for the great demonstration. I hope that we will be able to expose this to more people in the future. I really apologize, but I am already late for a meeting.

Mr. KLAUS. Thank you, Senator Kyl.

Chairperson FEINSTEIN. Thanks, Senator, very, very much.

Let me ask this question, Mr. Klaus: Do you know of any company that had an attack where the company provided information to the Government and that information was leaked?

Mr. KLAUS. No. I think it is more of a perception.

Chairperson FEINSTEIN. I think that these fears that companies have about information leaking out are really contraindicated by the record. I wonder why they continue to have them.

Mr. Gent, can you comment on that?

Mr. GENT. I share your concern. The companies that I work with seem to be paranoid against providing the Government with information, particularly commercially viable information. We have often put restrictions on any information released for, say, 9 days, any commercially viable information. So I think that is a whole area that needs to be investigated, particularly as it applies here.

We have had several incidents, though, that show this is improving. We have reported maybe 20 or 30 incidents of hacker activity on our systems to the FBI. The FBI is always responsive. They come out, but they are held back by some of the laws that I heard from the previous panel, where they really can't do anything when they find it. But they can buildup a data base and a log of——

Chairperson FEINSTEIN. You mean because it originates out of the country?

Mr. GENT. Either that or it doesn't have enough financial repercussions that they can demonstrate directly.

Chairperson FEINSTEIN. I see.

Mr. KLAUS. The other thing is I think the InfraGard has been beneficial. I know in Atlanta we have the InfraGard meetings and those have grown pretty large, and I think that has built up a lot of trust between having law enforcement there and the FBI there, as well as the commercial or private sector being able to interact and have a kind of personal relationship. Hey, we are running into this problem, how do we deal with this? Now that they have those

ties or that personal networking through InfraGard, I think that is going to help out a lot.

Chairperson FEINSTEIN. I think what is interesting is because there are so many leaks from Government, companies incorrectly thought that they should not provide cyberattack information to the government. I don't believe leaks are a problem in this area. I think all these agencies really understand the importance of this information and the national security questions that are involved and that there aren't going to be any leaks of sensitive information. Therefore, companies have so much to gain by providing this information about cyberattacks so that law enforcement can get to the root of the problem and so that we in Congress know what laws to change to enable us to deter this activity.

Cyber attack activity seems to be multiplying and getting more coordinated. If the White House just hadn't acted promptly. This Code Red worm would have taken down their whole database. Is that fair to say?

Mr. KLAUS. It would have taken down their connection to the Internet, yes.

Chairperson FEINSTEIN. But it wouldn't have affected their hard drive?

Mr. KLAUS. It depends on what is exposed to the Internet. When you go to whitehouse.gov, it is more of a Web site kind of just to give you education on the Web site. I don't think much of their internal stuff is exposed to the Internet.

If the attacker really wanted to bring down stuff, he could target some more critical infrastructure that supports that Internet and it would have a much more serious effect. Whitehouse.gov is probably more symbolic. The Web site itself doesn't contain a lot of sensitive information, but any system on the Internet that is sensitive would be affected by Code Red by just simply changing the attack addresses.

Chairperson FEINSTEIN. Any other comment, Mr. Gent?

Mr. GENT. Well, one other in regard to InfraGard. At the national level, through the NERC operating Committee we have what is called a CIP forum where we are attempting to get all interested parties, which would include the FBI and other agencies interested in this, together with all of the operating people across North America that are interested in these subjects. It is informal right now, but we are hoping that it will result in some standards being written and some processes and procedures put out there where somebody can say, well, what do I do to protect myself, and they at least have a checklist where they can start. Of course, the first might be to call a security expert, but at least we are starting to give stuff out like that.

Chairperson FEINSTEIN. That is terrific.

Well, thank you both very much. We appreciate it, and please feel free to keep in touch with us, both Senator Kyl and myself. If you have any further thoughts, please let us know. Thank you very much.

Let me thank the audience.

This hearing is adjourned.

[Whereupon, at 4:13 p.m., the Subcommittee was adjourned.]

[Submissions for the record follow:]

SUBMISSIONS FOR THE RECORD

Statement of Hon. Charles E. Grassley, a U.S. Senator from the State of Iowa

Today, we examine the progress of the National Infrastructure Protection Center (NIPC), and to what extent they are fulfilling their charter as set forth in Presidential Decision Directive-63. Let me first thank all of the panel members for taking time out of their busy schedules to be here today. And, I would also like to thank the Government Accounting Office for their hard work in preparing their report.

This is a time of extraordinary change. We sit here today in the midst of one of the most significant technological revolutions in the history of the world. With each passing day, we add to the dramatic expansion in computer capacity, most notably through the increase in the use of the Internet. This new medium has altered our society and our economy in many significant ways. The breathtaking technological advances led by the concept of free enterprise have left scarcely a corner of the globe untouched by this remarkable tool. And the day-to-day activities of business and government have become enmeshed in the use of computers and the Internet to an extent that would have been unthinkable even ten years ago.

The infrastructure foundations on which this nation depends are an extremely complex system of interrelated elements. And true to its free market roots, this has not been a jointly coordinated revolution. Each of these infrastructure elements have taken their own path to become the networks that they are today. And while each of these elements can also be viewed as islands unto themselves, they are all connected to each other and to the outside world by one common element: a telephone line. So, while we may be the most technologically advanced nation on earth, we are also the most technologically vulnerable.

Consequently, the issue of public-private cooperation has become essential to the success of the safeguarding of our national infrastructure. We cannot count on the federal government alone to protect our critical infrastructure from cyber-terrorism, because the government doesn't own or operate the networks that carry most of our critical content. The private sector is not only needed, but pivotal in this endeavor. Private industry owns 90 percent of the national infrastructure, yet our country's economic well-being, national defense, and vital functions depend on the reliable operation of these systems.

Cyber-Security and critical infrastructure protection are among the most important national security and economic issues facing our country today, and will only become more challenging in the years to come. Recent attacks on our infrastructure components have taught us that security has been a relatively low priority in the development of computer software and Internet systems. These attacks not only have disrupted electronic commerce, but have also had a debilitating effect on public confidence in the Internet.

Recognizing this vital need to coordinate the protection of our critical systems, the NIPC was formed pursuant to the 1998, Presidential Decision Directive. We are here today to review the performance of the NIPC relevant to that charter. To be frank, there is not much here for me to be optimistic about.

It is clear to me that the problems outlined within the GAO report are symptomatic of a mission that is incomplete in its conception. I would not take issue with those who advocate the position that many of the problems experienced by the NIPC can be attributed to a significant lack of definition within the PDD–63 charter. And, I am also mindful of the fact we are reviewing what some have termed as a "start-up" program that has only been in existence for three years. But I would suggest to you that the deficiencies noted by the GAO can also be attributed to a lack of operational capability. And that these problems are also symptomatic of a much larger issue within the NIPC, and the FBI in particular; that being the pervasive "culture of arrogance" within the bureau. One cannot underestimate the negative affect that this culture has had upon the ability of the NIPC to fulfill its mission.

One of the few areas in this report where the GAO offers some positive evaluation is in the FBI's coordination of investigations of attacks on "computer crimes". But I don't believe this assessment takes into account the cooperative spirit called for within the NIPC charter. Instead of being a focal point to coordinate the investigations of various federal law enforcement agencies, the NIPC has simply become a conduit for the FBI to fund its own computer crime cases. The internal culture of the bureau is not built on the culture of sharing information with fellow law enforcement agencies. The NIPC charter calls upon the bureau to distribute cases according to expertise. With very few exceptions, this is not being done. A significant number of participating agencies have withdrawn their participation, not only because all of the incoming cases have been taken by the FBI, but also because their

contributions and expertise have not been incorporated into the NIPC in any significant way. Consequently, the NIPC should not be held up as an example of success in the field of interagency cooperation.

By its very nature, the FBI does not share information, it restricts information. Getting the criminal is the FBI's first priority—warning the public is secondary. For example, the NIPC has been tasked by this Presidential Decision Directive to provide timely warnings, mitigate attack and monitor reconstitution efforts. But the mission doesn't stop there; it also includes providing comprehensive analyses to determine if an attack is underway, the scope and origin of the attack, and the coordination of the government's response. In the realtime confusion of a cyberattack, the NIPC will have to decide whether or not an incident is an attack which will impact national security, or a criminal act that will require a criminal investigation. These conflicting national responsibilities impede decisions and put the nation at risk. The FBI's methodology for investigating crimes is incompatible with the mission intended for the NIPC. And that is why we should not allow the FBI to further commandeer this program.

History has proven that the FBI cannot maintain effective partnerships within the federal government or even within their own federal law enforcement community. How can we then expect the bureau to establish effective partnerships with the private sector? Can we honestly expect that the widespread aversion within the private sector to entrust sensitive corporate information is any less assuaged by the FBI stewardship of this program? One answer can be found in the inability of the NIPC to establish successful sharing agreements with all but one of the Information Sharing and Analysis Centers. Further, the NIPC has failed to successfully establish either an adequate warning and analysis capability, or reconstitution design under the Key Asset Initiative—both crucial foundations of the charter. One approach that does appear to have acquired a successful constituency within the private sector is the InfraGuard Program, and I would encourage the continued expansion of this initiative.

In conclusion, I want to once again thank the General Accounting Office for their hard work on this report. But I want to be clear that I take issue with some of its conclusions regarding the PDD–63 framework. I would suggest that the deficiencies noted with the NIPC owe as much to the insular culture within the FBI than to the number of mitigating factors ascribed by the GAO. Our nations critical security and infrastructure programs are currently under executive review. I look forward to this evaluation and to working with the relevant parties to improve the protection of our nations critical computer-dependent infrastructures.

Statement of Eugene F. Gorzelink, Director, North American Electric Reliability Council, Washington, DC

My name is Eugene F. Gorzelnik, and I am the Director—Communications for the North American Electric Reliability Council (NERC). Part of my job since the late 1980s is to facilitate NERC's activities within the industry and with the federal government as these activities relate to terrorism and sabotage of the electric systems of North America. Since mid-1998, these activities include critical infrastructure protection. I report directly to the President and CEO of NERC in these matters.

NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. It works with all segments of the electric industry—investorowned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; and power marketers—as well as customers to "keep the lights on" by developing and encouraging compliance with rules for the reliable operation of these systems. NERC comprises ten Regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

In my testimony I will discuss several related critical infrastructure protection programs that NERC participates in: Critical Infrastructure Protection Working Group (CIPWG); Indications, Analysis, and Warnings Program; Electricity Sector Information Sharing and Analysis Center (ES–ISAC); Critical Infrastructure Protection Planning; and Partnership for Critical Infrastructure Security.

SUMMARY

The North American Electric Reliability Council (NERC) and the electric industry worked closely with the National Infrastructure Protection Center (NIPC) for about

two years to develop a voluntary, industry-wide physical and cyber security indications, analysis, and warning (IAW) reporting procedure. This program provides NIPC with information that when combined with other intelligence available to it will allow NIPC to provide the electric industry with timely, accurate, and actionable alerts and warnings of imminent or emerging physical or cyberattacks. A high degree of cooperation with NIPC is possible because the industry has a long history of working with local, state, and federal government agencies. In addition, the NERC Board of Trustees in the late 1980s resolved that each electric utility should develop a close working relationship with its local Federal Bureau of Investigation (FBI) office, if it did not already have such a relationship. The Board also said the NERC staff should establish and maintain a working relationship with the FBI at the national level.

The IAW reporting procedure is modeled on an existing electric system disturbance reporting procedure in which electric utilities report system disturbances meeting a predefined criteria to the U.S. Department of Energy. A pilot IAW program was field tested in one NERC Regional Reliability Council in the fall of 1999 and winter 1999/2000. The program was refined and rolled out to the industry via three workshops held during the fall of 2000 and winter 2000/2001. A comprehensive communications program is being developed to bring this program to the attention of those industry entities that were not able to participate in the workshops.

NERC is satisfied with the working relationship it has with NIPC.

INTRODUCTION

NERC has served on a number of occasions during the past decade as the electric utility industry (electricity sector) primary point of contact for issues relating to national security. Since the early 1980s, NERC has been involved with the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multisite sabotage and terrorism, Year 2000 rollover impacts, and now the threat of cyber terrorism. At the heart of NERC's efforts has been a commitment to work with various federal government agencies such as the U.S. National Security Council, U.S. Department of Energy (DOE), and FBI to reduce the vulnerability of interconnected electric systems to such threats.

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

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison, worked through its Infrastructure Assurance Outreach Program to perform an information assurance assessment for a small number of nodes on NERC's industry information system. The purpose of this assessment was to help NERC and the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. A second follow-on information system assessment was begun in late 2000 and will be completed shortly. The product of this study will be recommendations that will form the basis of a draft NERC policy on information assurance. In addition, to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America, DOE has provided clearances for a number of industry personnel and clearances for other key industry personnel are anticipated. These clearances compliment those obtained from the Federal Bureau of Investigation (FBI) as a result of encouragement by NIPC, as discussed below.

CRITICAL INFRASTRUCTURE PROTECTION WORKING GROUP (CIPWG)

After several exploratory scoping sessions with DOE and NIPC, NERC created a Critical Infrastructure Protection (CIP) Forum to evaluate sharing cyber and physical incident data affecting the bulk electric systems in North America. The meetings of this group were widely noticed and the participants included all segments of the electric utility industry and representatives from several government agencies including the Critical Infrastructure Assurance Office (CIAO) of the Department of

Commerce, DOE, and NIPC. As a result of the groups' deliberations, NERC created a permanent group within the NERC committee structure—the Critical Infrastructure Protection Working Group (CIPWG). This working group reports to NERC's Operating Committee. It has Regional Reliability Council and industry sector representation as well as participation by the CIAO in the Department of Commerce, DOE, and NIPC.

INDICATIONS, ANALYSIS, AND WARNINGS PROGRAM

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

The electric industry Indications, Analysis, and Warnings Program, which evolved from this work (Attachment A), was presented to the NERC Operating Committee in July 2000 for discussion and approval. The Operating Committee approved a motion to implement the program; initial emphasis is on reporting by security coordinators and control areas. Individual electric utilities, marketers, and other electricity supply and delivery entities are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings and related materials. Workshops were conducted during the fall 2000 and winter 2001 to provide program details to the industry. A more comprehensive communications program is being developed by CIPWG to encourage broader industry participation in the program.

NERC views the Indications, Analysis, and Warnings Program as a voluntary first step toward preparing the electricity sector to meet PDD–63 objectives.

ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS CENTER (ES–ISAC)

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

The CIPWG has endorsed, and NERC has accepted, the naming of NERC as the Electricity Sector Information Sharing and Analysis Center (ES–ISAC). The functions performed are essentially the same as those functions that have been required of NERC for physical sabotage and terrorism. The ES–ISAC's duties are:

1. Receive voluntarily supplied incident data from electric industry entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.
3. Assist the NIPC personnel during its analyses on a cross private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts and other related materials to all those within the electric industry who wish to participate.

The ES–ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will likely request support for a 24-hour, seven days a week staffed facility. To this end, NERC also is exploring the feasibility of forming a joint ISAC with other sectors.

NERC has established relationships with the other existing ISACs through the Partnership for Critical Infrastructure Security (see below) and will establish relationships with other ISACs as they form.

CRITICAL INFRASTRUCTURE PROTECTION PLANNING

The CIPWG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the electric industry (Attachment B). Separate business cases have been prepared for Chief Executive Offcers, Chief Operating Officers, Chief Information Officers, and a NERC general overview (Attachments C, D, E, and F). The purpose of the business case is to persuade industry participants of the need to report cyber intrusion incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPWG has developed a—basic and fairly comprehensive plan to address CIP. The working group was concerned about generating an overly prescriptive plan too early in the process and has proceeded with a format that can assist in developing each entity's own plan. The prototype plan, which still is undergoing industry review, addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, reconstitution, and interdependencies between and among sectors.

The essence of this "Approach to Action" is being considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government. Richard Clarke, Special Assistant to the President and National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, has discussed the importance of establishing and maintaining a National Plan to the health of the government and private sectors, companies, and the nation. Version 1.0 of the Plan did a good job covering the threats and the government response, but it did, not detail private sector response. The need for private sector participation is engendered by the fact that the government lacks private sector expertise and needs private sector "buy in" to CIP initiatives. The National Plan version 2.0, which will include private sector input, is scheduled for fall 2001.

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

The Partnership for Critical Infrastructure Security (PCIS) was proposed in late 1999 by members of several private sectors; the PCIS is supported by CIAO and the U.S. Chamber of Commerce. Earlier this year, it established itself as a not-for-profit organization and elected a Board of Directors and company officers. NERC participates in PCIS and Michehl R. Gent, NERC's President and Chief Executive Officer, serves as PCIS' Secretary.

The PCIS Mission:

> Coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

The PCIS held two general forums in 2000 and one so far this year. It is planning a second general forum on September C–7, 2001. The PCIS has formed six active working groups: Interdependency Vulnerability Assessment and Risk Management; Information Sharing, Outreach and Awareness; Public Policy and Legislation; Research and Development and Workforce Development; Organization Issues and Public-Private Relations; and National Plan. The opportunities presented by PCIS include gaining a better perspective of the sector interdependencies, facilitating ISAC formation, and sharing of common research and development efforts.

Statement of Taher Elgamal, Chairman, President & CEO, Securify, Inc., Mountain View, CA

EXECUTIVE SUMMARY

Protecting our nation's critical infrastructures today is a great challenge given the open and global nature of the Internet. Since the Internet was not developed for commercial activity and since it does not recognize political borders, industry and government need to invest in new technologies and business practices in order to strengthen the Internet. Obviously more and more value resides online in networks. Increasingly, society itself is dependent upon computer-based communications and the Internet.

Greater coordination between governments and industry is necessary. Information sharing and analysis is a good start. However, security needs to become a tool for running one's business or organization in a more effective manner, rather than a reaction to a problem. Fundamentally, security is first about being aware of what

is actually happening on one's network. Simply putting up barriers at the perimeter of your network is not going to work. There are no walls in cyberspace: remote access by employees, consultants on site, and ever increasing interconnectedness with other networks eliminate any sense of walls. Rather than defending one's network from perceived outside threats, one must instead manage from the inside outward. Vigilance rather than repair will become the standard operating procedure for both industry and government networks.

INTRODUCTION

Protection of our nation's critical infrastructure requires increased attention from business and government. With the advent of the Internet more of society is dependent on computer-based communications. This will not change. Globalization, economic productivity, trade, innovation, education, and other drivers accelerate dependency. Since the private sector owns or operates the vast majority of the world's information infrastructure and relies upon other infrastructures (e.g., energy, law enforcement, health care, finance, transportation, defense) that are recognized in many cases as government driven, both industry and government must cooperate closely on the significant issues before the Subcommittee today.

Security,Inc., is pleased to be a witness. We believe that our approach to security enables business and government to be in a superior position to address today's infrastructure concerns. From my own professional experience I know first hand about the close working relationships between industry and government in the area of security. For example, my PhD thesis became the adopted DSS government standard for digital signatures. Based on this experience I respectfully suggest some public policy ideas for the Subcommittee to consider.

BACKGROUND ON SECURIFY, INC.

One cannot have security without the ability to continually verify that actual activity comports with expectations, rules and policies. One can spend a lot of time and money on people and technology and not improve the quality of security. Verification is an essential and logical first step.

Securify was founded in 1998 as VeriGuard, Inc. Within the first 10 months the company changed its name to Securify and was then sold to Kroll-O'Gara, a publicly traded risk mitigation and security services firm. Kroll-O'Gara spun Securify out as an independent company in 2000. Today Securify is a privately held firm with approximately 100 employees. Our headquarters are based in Mountain View, California.

Securify began as a high-end information security consulting firm. Clients were Fortune 50 firms with very sensitive security needs. Early on Securify recognized that customers needed automated, technology driven and continuous security solutions. Customer needs escalated and outstripped the availability of security experts and consumed increasing portions of IT budgets. A proactive, cost-effective approach that served the business needs of the customer was necessary. For nearly two years Securify has researched and developed a unique, patent-pending technology. It is called SecurVantage.

Securify designed this unique, managed service for measuring security effectiveness of business networks including intranets, production networks and connections to the networks of partners, customers and suppliers. Securify SecurVantage provides in-depth visibility and analysis of the security attributes of live network traffic, enabling security managers and IT staff to quickly detect misconfiguration, and the presence of unauthorized devices.

Most organizations manage each security device independently and hope the combination of devices provides security. Securify SecurVantage provides a continuous method for comparing real time traffic to business-level security standards. Performing this analysis of real time traffic on a continuous basis is the best method to ensure live traffic is conforming to corporate security guidelines. Securify SecurVantage provides a high-level overview of security policy development, implementation, and continuous maintenance. It quickly targets inconsistencies and recommends corrective actions. Securify SecurVantage establishes a baseline, customized, business-driven security policy specification for each customer. Using this specification, network traffic is analyzed for conformance to the desired security requirements. If a violation is detected, the Securify Network Operations Center (NOC) staff alerts the customer of the violation and recommends corrective action. Securify SecurVantage can also be used to establish metrics to ensure traffic flowing between business partners meets required security parameters. This is particularly important for companies that rely on their distributed networks for day-to-day operations, wherever valuable data is accessed and stored.

Securify's SecurVantage demonstrates the combination of security and verification. By continually verifying that the activity on your networks and the networks you connect to is what is expected, then one can focus on mitigating the deviations, anomalies, deviations and exceptions. This is a significantly smaller set of events to focus on than the ever evolving and growing universe of threats and vulnerabilities. Rather than reacting to the expanse of threats and vulnerabilities one can mitigate risk on a level that is customized and do so in an intelligent and managed manner. It is the difference between reacting on little or no information to acting according to a plan. And since this approach is a part of the every day functioning of the customer's business and their networks, they have the ability to assess security performance and other network attributes. So it is more than security; it helps make the network and the organization it serves healthier, more reliable and productive. It simply makes it more valuable.

This is an important point. Government and business increasingly have more value and more at stake digitally than physically. Assets and value are based not on material objects but on information assets and network connections. From General Electric to Dell, from old to new, more businesses are using technology to change how they're run and to manage their operations and relations with employees, customers, suppliers and partners.

More revenue is derived from network activity. More cost savings are gained from online activity. Today this is no longer headline news but a real fact of life for business and government alike.

We all recognize that an organization cannot function properly, effectively, successfully, competitively or legally without sound financial management processes and systems. A business cannot function if it does not continually know the status of money coming in and money going out and who it touching the money. The same has become true for network activity and the increasingly valuable and critical information that flows through the network. Even today, discussions of corporate network security issues are delegated down from corporate management to the IT department. Recent reports by the GAO on the status of government network operations reveal a similar problem. We believe that a healthy dialogue between senior government officials, corporate CEOs and Boards of Directors, academia and others is required if these issues are to be appropriately addressed and resolved.

As a vendor of security technology and solutions, Securify of course stands to benefit from spending on security by business and government. Securify is not here today to recite the latest statistics on the number of attacks and threats and their cost to business and our economy. Frankly, the damage done by overt activity is overshadowed by the costs resulting from poorly managed networks.

Securify advocates the adoption of the proactive and continuous approach of verification. It is simply good business and trustworthy government. One cannot manage what they do not measure. If one does not have a network security policy in place and if one does not continually measure the actual activity on the network against this policy, then one will never know if they are secure. As a result the network is unreliable and it cannot ensure privacy, security, and integrity.

It is important to note that the Internet was designed some thirty years ago by collaboration between government, industry and academia. The Internet was designed to be an open medium for sharing information. Security and commercial activity were not a part of the original programming. It is important to recognize this plain fact. Now that we are all dependent on the Internet and computer-based communications we need to take some new action to make the Internet strong enough.

Action includes increased information sharing and analysis within industry and government. Action includes adopting new technologies and business practices. Spending on security has not really diminished in the current economic climate. A recent survey of the chief information officers of the Fortune 100 reported that security spending is the last item to be cut from an IT budget. This may be stating the obvious. One does not cut what protects one's assets. What is not so obvious is that security spending has increased in recent years but no one really knows how effective those investments have been.

If one can start from the first point of a verified network then the owner and operator of that network has the ability to continually ensure that it is functioning within expected parameters. They can track activity and correct errors and analyze historical records for improvement and modification. Results of this include greater reliability (i.e., less network downtime), privacy assurance (i.e., one has the ability to determine if the set privacy rules and practices are being applied properly and fol-

lowed) and greater security (i.e., one can track deviations and anomalies in real time across all networks).

This is not some sort of big brother technology. It is a business tool. Just as a senior management team and a board of directors must know if there is a misuse of funds or property or some sort of illegal activity taking place inside their company, they must have the tools and ability to detect and mitigate the same sorts of unauthorized activity in the digital world. Such a tool provides for transparency in the operation of a business. Without it truly nefarious activity would be able to flourish and do so unchecked as no one would be readily able to detect it or mitigate it.

By using SecurVantage our customers immediately see unauthorized activity such as an employee using a file server to transmit sensitive data to a competitor. Employees and consultants use a network and its resources to run gambling and pornography businesses. Many misuse their access to peruse parts of the network they don't need to see or should not gain access to. These are just a few examples. But they easily illustrate the costs of misuse of a network. From just the cost control perspective, network misuse increases operating costs. Why should a company pay for more bandwidth, energy, equipment or technical support than it has to in order to do its business? Again, security is really about running an organization correctly and effectively. It is not simply a matter of preventing attacks or locking secrets away. At some point, financial audits are less than complete if a company's network security vulnerabilities and practices are not reviewed and discussed, especially for certain types of firms. Any company involved in an acquisition today would want to investigate the target company's network security practices as an ordinary due diligence item.

WHAT THIS MEANS FOR THE PUBLIC POLICY LANDSCAPE: NEW ACTIVITY FOR POLICY MAKERS

The Administration recently announced its intention to change the approach of government on managing security and critical infrastructure policymaking functions. A fresh approach that accounts for the increasing significance of the issues is most welcome. Securify is involved in many government and industry groups. From the G8 to the OECD to the Council of Europe to the US Congress to the European Commission to the Japanese Government, there is, government driven activity. From the Global Business Dialogue on Electronic Commerce (GBDe), to various industry trade associations to the newly created information sharing and analysis centers (ISACs) for key industry sectors (e.g., IT, transport, energy, finance), there is increasing senior executive level attention to these issues.

10

Industry remains sensitive to control of technical standards and open, global markets. Governments remain interested in setting some parameters for best practices and liability for criminal activity. Some in industry fear sharing information in industry groups as an exposure to one's competitors and to attackers. Some in industry fear sharing information with government will lead to an unauthorized disclosure and possible public embarrassment and perhaps litigation. Multinational companies and some governments wonder how information sharing and analysis can cross borders when trust between parties may not be sufficient to address national security and espionage concerns. Many government officials and Members of Congress are concerned about foreign ownership of sensitive technologies developed here in the United States (e.g., Verio-NTT, VoiceStream-Duetsche Telekom, Silicon Valley Group-ASM Lithography (ASML), Lucent-Alcatel).

Law enforcement of course needs to have lawful access to data. Cooperation between governments and companies across borders is critical. As information sharing and analysis cooperation between government agencies and industry groups grows in the US, we will need to focus on the issue of sharing across borders. This is not a radical idea. Indeed, we can learn from our past.

Some sixty-five years ago academics, mathematicians, government intelligence specialists, cryptographers, chess masters, and others from several countries quietly