S. HRG. 106–1092

INTERNET SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MARCH 8, 2000

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

78–382 PDF WASHINGTON : 2003

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
SLADE GORTON, Washington	JOHN D. ROCKEFELLER IV, West Virginia
TRENT LOTT, Mississippi	JOHN F. KERRY, Massachusetts
KAY BAILEY HUTCHISON, Texas	JOHN B. BREAUX, Louisiana
OLYMPIA J. SNOWE, Maine	RICHARD H. BRYAN, Nevada
JOHN ASHCROFT, Missouri	BYRON L. DORGAN, North Dakota
BILL FRIST, Tennessee	RON WYDEN, Oregon
SPENCER ABRAHAM, Michigan	MAX CLELAND, Georgia
SAM BROWNBACK, Kansas	

MARK BUSE, *Policy Director*
MARTHA P. ALLBRIGHT, *General Counsel*
KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

CONRAD BURNS, Montana, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
SLADE GORTON, Washington	DANIEL K. INOUYE, Hawaii
TRENT LOTT, Mississippi	JOHN F. KERRY, Massachusetts
JOHN ASHCROFT, Missouri	JOHN B. BREAUX, Louisiana
KAY BAILEY HUTCHISON, Texas	JOHN D. ROCKEFELLER IV, West Virginia
SPENCER ABRAHAM, Michigan	BYRON L. DORGAN, North Dakota
BILL FRIST, Tennessee	RON WYDEN, Oregon
SAM BROWNBACK, Kansas	MAX CLELAND, Georgia

CONTENTS

WITNESSES

APPENDIX

INTERNET SECURITY

WEDNESDAY, MARCH 8, 2000

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:35 a.m. in room SR–253, Russell Senate Office Building, Hon. Conrad Burns, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. The Subcommittee on Communications of the Commerce, Science, and Transportation Committee will come to order. First, I would like to welcome everyone to today's hearing, which is the first of a series of hearings that this Subcommittee will hold on the critical issues of Internet security and privacy facing our Nation.

Today's hearing will focus on the unprecedented and apparently coordinated recent series of hacker attacks which caused some of the most popular Web sites on the Internet to go dark. The list of sites that were brought down include such Internet mainstays as Amazon.com, eBay, my Auction Barn was shut down, no telling how much money it cost me——

[Laughter.]

Senator BURNS. —cnn.com and e-Trade and Yahoo.

These attacks are technically called "distributed denial of service attacks," which in plain English is like a telephone system getting overwhelmed by more calls than it can handle. It appears the hackers planned their attacks months in advance, going so far as to set up software on many servers all over the Internet that was capable of automatically flooding targeted Web sites at a certain predetermined time.

I suppose it is no surprise that these malicious programs are called "daemons," spelled d-a-e-m-o-n-s. The hackers involved in these attacks have yet to be caught, despite the coordinated efforts of our Nation's top law enforcement agencies.

While no consumer data was stolen, real damage was done, especially to Internet user's confidence about the security systems that they are using. The fear of future attacks was enough to cause a massive sell-off in technology stocks in early February, when the attacks took place, and the nature of these attacks is particularly alarming, as they were specifically designed to disrupt electronic commerce.

The growth of electronic commerce and the Internet has been generally astounding. The number of small businesses on the Web is doubling every year, and currently over 2 million small businesses in the United States have Web sites. In my home State of Montana, companies such as Vanns.com and Streaming Solutions are showing that all their great work and great ideas are coming to fruition. E-commerce potential of the Internet still has tremendous up-side, while household spending online last year doubled. It is still only about 1 percent of the total retail dollars.

The growth in the Internet is a double-edged sword, however. Unfortunately we now live in a world where there are malicious criminals who can bring large parts of our Nation's critical information infrastructure to a grinding halt. Given the seriousness of these attacks, we must act not only quickly but effectively. We must think it out and work in the best way. In other words, we cannot out-force our enemies. We must out-think them and be smarter than they are.

We need to do everything possible to foster better coordination between Government and industry in protecting Internet security, make sure that our national security and our law enforcement agencies have the resources to do their job, and to bring our Nation's criminal code up to date with the recent development of the Internet. Clearly, the current level of coordination between Government agencies and the private sector needs to be as seamless and effective as possible.

A core component of achieving this cooperation is the continuing development of the FBI's National Infrastructure Protection Center, which was set up 2 years ago to deal with the range of potential attacks on the Internet. I strongly supported the creation of that center, and I will continue to support its full funding. In fact, I want to make it even stronger.

I am concerned, however, that the center is authorized for 133 employees. We are only up to about 100 now, 40 of whom are detailees from other agencies, but I also understand the FBI is still short of its goal of hiring 250 field agents to fight cybercrime. While I realize that hiring top-level technical experts to work in Government is difficult, given the lure of Silicon Valley, these positions need to be filled as quickly as possible, and that is what I have always argued in the past, and I want to make a comment on that this morning.

Instead of putting a lid on technology we need to fully fund and fully support our law enforcement agencies so they are abreast of or half a step ahead and working with industry in the technology so they can get their job done, so we need a lot of work, and I am going to put the rest of my statement in here, because I do want to hear from witnesses this morning.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

I would like to welcome everyone to today's hearing, which is the first in a series of hearings this Subcommittee will be holding on the critical issues of Internet security and privacy facing our nation. Today's hearing will focus on the unprecedented and apparently coordinated recent series of hacker attacks which caused some of the most popular websites on the Internet to go dark. The list of sites that were brought

down included such Internet mainstays as Amazon.com, eBay, cnn.com, e-Trade and Yahoo.

These attacks are technically called "distributed denial of service attacks" which in plain English is like a telephone system getting overwhelmed by more calls than it can handle. It appears the hackers planned their attacks months in advance, going so far as to set up software on many servers all over the Internet that was capable of automatically flooding targeted websites at certain predetermined times. I suppose it's no surprise that these malicious programs are called "daemons." The hackers involved in theses attacks have yet to be caught, despite the coordinated efforts of our nation's top law enforcement agencies.

While no consumer data was stolen, real damage was done-especially to Internet users' confidence about the security of the systems they are using. The fear of future attacks was great enough to cause a massive selloff in technology stocks in early February when the attacks took place. The nature of these attacks is particularly alarming, as they were specifically designed to disrupt electronic commerce.

The growth of electronic commerce and the Internet in general has been astounding. The number of small businesses on the Web is doubling every year, and currently over 2 million small businesses in the United States have websites. In my home state of Montana, companies such as Vanns.com and Streaming Solutions are showing that all it takes is a great idea and hard work to reach global markets through the Internet. The e-commerce potential of the Internet still has tremendous upside—while household spending online doubled last year, it still amounted to less than 1 percent of total retail dollars.

The growth and reach of the Internet is a double-edged sword, however. Unfortunately, we now live in a world where malicious criminals can bring large parts of the nation's critical information infrastructure to a grinding halt.

Given the seriousness of these attacks, we must act quickly and effectively. We need to do everything possible to foster better coordination between Government and industry in protecting Internet security, make sure our national security and law enforcement agencies have the resources to do their jobs and bring our nation's criminal code up-to-date with the recent development of the Internet.

Clearly, the current level of coordination between Government agencies and the private sector needs to be as seamless and effective as possibe. A core component in achieving this cooperation is the continuing development of the FBI's National Infrastructure Protection Center, which was setup two years ago to deal with a range of potential attacks on the Internet. I strongly supported the creation of the Center and continue to support its full funding.

However, I am concerned that while the Center is authorized for 133 employees, its staff is still at only 100, 40 of whom are detailees from other agencies. I also understand the FBI is still short of its goal of hiring 250 field agents to fight cybercrime. While I realize that hiring top-level technical experts to work in the Government is difficult given the lure of Silicon Valley, these positions need to be filled as quickly as possible.

I want to touch on the issue of criminal penalties on hackers. In the recent past, many if not most "hacker" attacks were the product of intellectual curiosity rather than malicious intent to cause damage. Now, however, the vast majority of hacker attacks are done through simply downloading pre-existing programs from hacker sites on the web and using them to accomplish destructive aims. Rather than stemming from misdirected teenage rebellion, current attacks are often engaged in by adults who want to inflict the most damage possible. We need to severely punish these criminals-and they are criminals. The destruction of data belonging to innocent individuals is no less a crime than property destruction of the more traditional type. In fact, it can in many cases be far worse.

We are fortunate to have some of the foremost Government and industry experts in the field of Internet security with us today. I look forward to the testimony of the witnesses in addressing these matters of critical importance to the continued development of e-commerce and the Internet. Thank you.

Senator BURNS. We are joined this morning by Senator Hollings. Thank you for coming.

STATEMENT OF HON. ERNEST F. HOLLINGS, U.S. SENATOR FROM SOUTH CAROLINA

Senator HOLLINGS. Thank you, Mr. Chairman. If I heard you correctly, you said we are going to have to be smarter than they are. If we wait on Government to be smarter, that is quite a charge.

Senator BURNS.We are not asking for the impossible.

Senator HOLLINGS. That is near it. We are back—history repeats itself. You have got to think of David Sarnoff on the Wannamaker Building and the sinking of the LUSITANIA. He picked it up. The country went wild over wireless, and by the mid-twenties everybody was jamming. Everybody in the so-called free market of communications came crying to Government, please regulate us. Now history repeats itself. They come crying to Government, please give us security, please give us privacy, because they cannot do it themselves. They say it takes two to tango. You cannot have privacy without security.

So the Justice Department has been working diligently and I might add, Mr. Chairman, the Justice Department has grown quite a bit in recent years. Slightly over 10 years ago the budget in the Justice Department was $4 billion. It is now $23 billion. Everybody says cut spending, cut spending, cut spending, but the Senators ought to know we have been increasing it like gangbusters, and giving the Justice Department everything they say they can possibly use, and they have been doing an outstanding job.

In essence, the National Institute of Standards and Technology is really onto the technology, and I am delighted to hear from the witnesses, and I would ask the remainder of my statement be included.

[The prepared statement of Senator Hollings follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Senator Burns, thank you for holding this hearing today. It is the first hearing in a series that the Committee intends to hold on the subject of electronic privacy.

Internet security and hacking are not generally discussed in the context of privacy, but I think that this is an important first topic for consideration. No matter what we decide on the right policy to protect consumers on the Internet is, no policy can work without a secure infrastructure. A company can have the strongest privacy policy in the world, but that policy is irrelevant if the company has not adequately protected its systems from illegitimate users.

A month ago at this time, Mr. Misener's company, among others, was under attack. That attack highlighted problems which have plagued the users of the Internet for some time. Having been brought under the media spotlight the question now is: How can we be sure that the companies we are doing business with on the Internet are secure? Additionally, what do businesses owe their consumers when they are victims of computer break in?

In order to make consumer information safe from hackers, it will be necessary to raise the security standards of Internet-based businesses as a whole. As we try to craft public policy in this area, we need to examine three constructive roles for Government: (1) fostering constructive partnerships which enhance private sector security; (2) pushing the technological envelope on information infrastructure protection; and (3) being a role model through the implementation of best security practices.

In other words, the Government must be prepared to form a partnership with industry to share information on new attacks and how to stop them. Our research agencies must invest in solving problems which will bolster the security of the whole Internet rather than its parts. Finally, the Government needs to do a better job of protecting its own information. Right now, our departments and agencies are far from a shining example of what Internet security can be. We need to have in place the right policies, hardware, software, and trained personnel to secure Government computer systems. I hope that our witnesses will address these areas in their testimony today.

Already, various agencies of the U.S. Department of Commerce are doing important computer security work. Undersecretary Reinsch oversees the Critical Infrastructure Assurance Office (CIAO) which is coordinating partnerships with the private sector to examine attack prevention. The National Institute of Standards and Technology (NIST) is a leader in computer security research and, through the 1987

Computer Security Act, sets standards for securing unclassified Government computer systems. The FY 2001 budget request for information security would enhance these capabilities at Department of Commerce and in other agencies of Government.

Again, I look forward to hearing the testimony of today's witnesses on how we can improve Internet security in this nation and what the role of the Government should be in achieving that goal.

Senator BURNS. Thank you, Senator Hollings. Senator Bryan.

STATEMENT OF HON. RICHARD H. BRYAN, U.S. SENATOR FROM NEVADA

Senator BRYAN. Mr. Chairman, thank you very much for convening this important and timely hearing this morning. As Vice Chairman of the Intelligence Committee, we are very much aware of the importance, in terms of our national security concerns, of computer hacking. All of us have been mindful of the recent successful attacks against some of the most significant Web sites in the country, and so I will be looking forward to hearing the testimony of our distinguished witnesses this morning. I would ask unanimous consent that the rest of my statement be made a part of the record.

Senator BURNS. Without objection, it sure will.

[The prepared statement of Senator Bryan follows:]

PREPARED STATEMENT OF HON. RICHARD H. BRYAN, U.S. SENATOR FROM NEVEDA

As our society continues to become more reliant on the Internet to conduct our daily affairs, the issue of Internet security becomes increasingly important for both the public and private sector. As Vice Chairman of the Intelligence Committee, I am very familiar with the national security concerns confronting our intelligence community on a daily basis that result from computer hacking. And as public agencies at all levels of Government continue to do more and more of their business online, Internet security becomes a paramount issue for Government officials. I look forward to hearing from our Government witnesses today, especially Deputy Attorney General Holder, on what additional law enforcement tools and other measures are needed to protect the integrity of the Federal Government's computer systems.

The recent denial of service attacks against a handful of the top U.S. web sites was a good illustration of the vulnerabilities faced by the private sector. Perhaps even more alarming, however, are the privacy concerns associated with security breaches for companies that gather large amounts of personally identifiable information about consumers over the Internet. The issues related to online privacy and Internet security are clearly interrelated, and I look forward to hearing our witnesses comment on what role the Federal Government should play in these areas.

Senator BURNS. Our first panel this morning is Mr. Eric Holder, Deputy Attorney General, U.S. Department of Justice, Mr. William Reinsch, Under Secretary of Commerce for Bureau of Export Administration, Department of Commerce, and Michael Vatis, Deputy Assistant Director, Federal Bureau of Investigation here in Washington, D.C.

Gentlemen, we welcome you to the table this morning. We look forward to your testimony, and the dialog that we may present this morning on this subject, and I will just start as they are listed. Mr. Holder, thank you for coming this morning. We look forward to your testimony.

STATEMENT OF ERIC HOLDER, JR., DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. HOLDER. Thank you, Mr. Chairman, Senator Hollings, Senator Bryan, other members of the Subcommittee. I want to thank

you for the opportunity to testify on cybercrime, including the recent Internet denial of service attacks. The Department appreciates the support we have received from Congress in providing significant resources and tools we need to keep pace with the ever-changing kind of cybercrime. We look forward to continuing our cooperation with Congress to ensure that law enforcement, in cooperation with the private sector—and that is very key, in cooperation with the private sector, play an appropriate role in protecting American citizens and businesses against cyber attacks while also safeguarding the privacy rights we hold dear in our country.

I would be happy to address your questions on the recent attacks to the extent that I can without compromising our investigation. At this point, I would simply say we are taking the attacks very seriously, and that we will do everything in our power to identify those who are responsible and to bring them to justice.

We are making, I think, progress in the investigation, and in addition to the malicious disruption of the legitimate commerce, so-called disruption attacks, they also involve the unlawful intrusion into a number of computers. Thus, the number of victims in these types of cases can be substantial, and the loss and cost to respond to those attacks can run into the tens of millions of dollars or more.

Computer crime investigators in a number of FBI field offices and investigators from other agencies are investigating these attacks. The agents are also working closely with our network of specially trained computer crime prosecutors who are available 24 hours a day, 7 days a week to provide legal advice and to obtain whatever court orders are necessary. We are also obtaining information from victim companies and security experts who, like many in the Internet community, condemn these recent attacks.

Now, while the Internet is providing wonderful benefits that are transforming our society and countless beneficial ways, from providing new high-wage jobs to our economy, to improving health care, and in countless other ways, these wonderful technologies also provide new opportunities for criminals.

Online crime is rapidly increasing. We are seeing more pure computer crime, that is, crimes where the computer is used as a weapon to attack other computers, as we saw in the distributed denial of service attacks I just spoke about, and in the spread of malicious codes like viruses. These crimes not only affect our financial well-being and our privacy, they also threaten our Nation's critical infrastructure.

We are also seeing a migration of traditional crimes, including threats, child pornography, fraud, gambling, and extortion from the physical to the online world. When these crimes are carried out online, perpetrators often find that they can reach more victims quickly and quite easily, turning what were once local scams into crimes that cross interstate and even international borders.

Now, while the Internet has tremendous benefits to our society, including greater freedom of expression and economic growth, we must also recognize that investigators and prosecutors at all levels, international, Federal, State, and local, are encountering unique challenges, and these include technical challenges that hinder law enforcement's ability to find and to prosecute criminals operating online, legal challenges resulting from laws, and legal tools needed

to investigate cybercrime lagging behind technological, structural, and social changes.

And third, we face resource challenges that limit our ability to focus adequate investigative, prosecutorial, and technical resources on cybercrime. Now, in this regard, the Department is seeking an additional $37 million in fiscal year 2001 to bolster our cybercrime program, including additional resources for the FBI, specially trained cyber prosecutors and assistants to State and local law enforcement agencies, but we recognize that Government will not be able to solve all of these problems.

In fact, we believe that the private sector should take the lead in protecting private computer networks through more vigilant security efforts, information-sharing and, where appropriate, cooperation with Government agencies. The private sector can and should take the lead when improving security practices, and the development of a more secure Internet infrastructure.

Now, despite the technical, legal, and resource challenges we face, the Department has made, we believe, strides in our fight against cybercrime. We have and we will continue to develop extensive investigatory and prosecutorial programs to counter cybercrime. We have established the FBI's National Infrastructure Protection Center, NIPC as we call it, and specialized squads located in 16 field offices. From the prosecutorial side, we have trained attorneys both at headquarters and in the field who are experts in legal technological and practical challenges involved in investigating and prosecuting cybercrime.

As a result of these programs, the number of cases and prosecutions by the Department is growing at a tremendous rate. For example, in 1998, U.S. Attorneys Offices filed 85 computer crime cases against 116 defendants, and this represents a 29-percent increase in the number of cases filed and a 51-percent increase in the number of defendants compared to the previous year. From the same period of time a total of 62 cases against 72 defendants were terminated, with 78 percent of those defendants being convicted.

On behalf of the Department, I again want to thank Congress for the support it has given to our efforts to combat cybercrime. Advancements in technology indicate that our efforts are really only just beginning. We look forward to working with Congress and the private sector to ensure that we have a robust and effective long-term plan for combatting cybercrime, protecting our Nation's infrastructure, safeguarding privacy, and ensuring the Internet reaches its full potential for expanding communications, facilitating commerce, and bringing countless other benefits to our society.

I look forward to responding to your questions.

[The prepared statement of Mr. Holder follows:]

PREPARED STATEMENT OF ERIC HOLDER, JR., DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. Chairman, Senator Hollings, and other Members of the Subcommittee, I want to thank you for this opportunity to testify on the recent Internet "denial of service" attacks and the Federal response to these incidents, with a particular focus on the challenges facing the Department of Justice in its fight against cybercrime. At a time where new technologies abound and our society becomes increasingly reliant on computer networks and thus vulnerable to cybercrime, we look forward to working with Congress to ensure that law enforcement, in cooperation with the private

sector, can play an appropriate and critical role in protecting the well-being of Americans while also respecting fundamental notions of individual privacy that we hold dear in this country.

Comments on the Recent Attacks

I would be happy to address your questions on the recent attacks, to the extent I can do so without compromising our investigation. At this point, I would simply say that we are taking the attacks very seriously and that we will do everything in our power to identify those responsible and bring them to justice. In addition to the malicious disruption of legitimate commerce, so-called "denial of service" attacks involve the unlawful intrusion into an unknown number of computers, which are in turn used to launch attacks on the eventual target computer, in this case the computers of Yahoo, eBay, and others. Thus, the number of victims in these types of cases can be substantial, and the collective loss and cost to respond to these attacks can run into the tens of millions of dollars—or more.

Overview of Investigative Efforts and Coordination

Computer crime investigators in a number of FBI field offices and investigators from other agencies are investigating these attacks. They are coordinating information with the National Infrastructure Protection Center (NIPC) of the FBI. The agents are also working closely with our network of specially trained computer crime prosecutors who are available 24 hours a day/7 days a week to provide legal advice and obtain whatever court orders are necessary. Attorneys from the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) are coordinating with the Assistant United States Attorneys in the field. We are also obtaining information from victim companies and security experts, who, like many in the Internet community, condemn these recent attacks. We are also working closely with our counterparts in other nations. I am proud of the efforts being made in this case, including the assistance we are receiving from a number of Federal agencies.

The Emergence of Cybercrime

It is worth remembering that just ten years ago, the Internet was largely unknown and unavailable to the average person. There was no e-commerce, no eBay, no Amazon.com. At that time, the Internet was a collection of military, academic, and research networks serving a small community of trusted users. That world is history. The far-reaching, ever-expanding, and ever more rapid advances in computer and software technology over the last ten years have combined with the explosive growth of the Internet to change the world forever. For the most part, the Internet and other technologies are providing wonderful benefits to our society—from providing new, high-wage jobs to our economy, to expanding educational opportunities, improving health care, and allowing family and friends to keep in touch in ways that were simply impossible a decade ago.

Unfortunately, these wonderful technologies also provide new opportunities for criminals. Online crime is rapidly increasing. We are seeing more "pure" computer crimes, that is, crimes where the computer is used as a weapon to attack other computers, as we saw in the distributed denial of service attacks I just spoke about, and in the spread of malicious code, like viruses. Our vulnerability to this type of crime is astonishingly high—it was only this past December that a defendant admitted, when he pled guilty in Federal and state court to creating and releasing the Melissa virus, that he caused over 80 million dollars in damage. These crimes also include computer intrusions designed to obtain information of the most sensitive sort—such as credit cards, companies' trade secrets, or individuals' private information.

These crimes not only affect our financial well-being and our privacy; they also threaten our nation's critical infrastructure. Our banking system, the stock market, the electricity and water supply, telecommunications networks, and critical Government services, such as emergency and national defense services, all rely on computer networks. For a real-world terrorist to blow up a dam, he would need tons of explosives, a delivery system, and a surreptitious means of evading armed security guards. For a cyberterrorist, the same devastating result could be achieved by hacking into the control network and commanding the computer to open the floodgates.

We are also seeing a migration of "traditional" crimes—including threats, child pornography, fraud, gambling, and extortion—from the physical to the online world. When these crimes are carried out online, perpetrators often find that the can reach more victims quickly and quite easily, turning what were once "local" scams into crimes that cross interstate and international borders. Computers and computer networks provide a cheap and powerful means of communications, and criminals

take advantage of this just like everyone else. In addition, sophisticated criminals can readily use the easy anonymity that the Internet provides to hide their crimes.

Challenges of Cybercrime

The Internet and computers have brought tremendous benefits to our society, including greater freedom of expression and economic growth. But we must also recognize that as a result of our society's increasing reliance on technology, investigators and prosecutors at all levels—international, Federal, state, and local—are encountering unique challenges. These challenges generally can be divided into three categories:

(1) *Technical challenges* that hinder law enforcement's ability to find and prosecute criminals operating online;
(2) *Legal challenges* resulting from laws and legal tools needed to investigate cybercrime lagging behind technological, structural, and social changes; and
(3) *Resource challenges* to ensure we have satisfied critical investigative and prosecutorial needs at all levels of Government.

Before I discuss each of these challenges, let me say that we recognize that we in Government will not be able to solve all of these problems. In fact, we believe strongly that *the private sector should take the lead in protecting private computer networks, through more vigilant security efforts, information sharing, and, where appropriate, cooperation with Government agencies.* The private sector has the resources, the technical ability, and the trained personnel to ensure that, as technology continues to develop and change rapidly, the Internet is a safer place for all of us. The private sector can and should take the lead on improving security practices and the development of a more secure Internet infrastructure.

However, even assuming that private sector, and the broader Internet community as a whole, take steps to provide a safe, secure, and vibrant Internet, there will be instances where the practices and safeguards fail. Criminals rob banks even though banks use numerous security measures. In such cases, law enforcement must be prepared and equipped to investigate and prosecute cybercriminals in order to stop their criminal activity, to punish them, and to deter others who might follow the same path. This is the reason that it is so important that we work together to address the challenges I am about to discuss.

Technical Challenges

When a hacker disrupts air traffic control at a local airport, when a child pornographer sends computer files, when a cyberstalker sends a threatening e-mail to a public school or a local church, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. Everything on the Internet is communications, from an e-mail to an electronic heist. Finding an electronic criminal means that law enforcement must determine who is responsible for sending anelectronic threat or initiating an electronic robbery. To accomplish this, law enforcement must in nearly every case trace the "electronic trail" leading from the victim back to the perpetrator.

Tracking a criminal online is not necessarily an impossible task, as demonstrated last year when Federal and state law enforcement agencies were able to track down the creator of the Melissa virus and the individual who created a false Bloomburg News Service website in order to drive up the stock price of PairGain, a telecommunications company in California. In both cases, technology enabled us to find the individuals who were engaging in criminal activity.

Unfortunately, despite our successes in the Melissa and PairGain cases, we still face significant challenges as online criminals become more sophisticated, often wearing the equivalent of Internet electronic gloves to hide their fingerprints and their identity.

It doesn't take a master hacker to disappear on a network. Ironically, while the public is justifiably worried about protecting the legitimate electronic privacy of individuals who use networks, a criminal using tools and other information easily available over the Internet can operate in almost perfect anonymity. By weaving his or her communications through a series of anonymous remailers; by creating a few forged e-mail headers with powerful, point-and-click tools readily downloadable from many hacker web sites; or by using a "free-trial" account or two, a hacker, online pornographer, or web-based fraud artist can often effectively hide the trail of his or her communications.

As we consider the challenge created by anonymity, we must also recognize that there are legitimate reasons to allow anonymity in communications networks. A whistleblower, a resistance fighter in Kosovo, a battered woman's support group—

all of these individuals may understandably wish to use the Internet and other new technologies to communicate with others without revealing their identities.

In addition to problems related to the anonymous nature of the Internet, we are being challenged to investigate and prosecute criminals in an international arena. The Internet is a global medium that does not recognize physical and jurisdictional boundaries. A criminal no longer needs to be at the actual scene of the crime to prey on his or her victims. As a result, a computer server running a web page designed to defraud U.S. senior citizens might be located in Europe or Asia. A child pornographer may distribute photographs or videos via e-mail, sending the e-mails through the communications networks of several countries before they reach their intended recipients. With more than 190 Internet-connected countries in the world, the coordination challenges facing law enforcement are tremendous. And any delay in an investigation is critical, as a criminal's trail might, in certain circumstances, end as soon as he or she disconnects from the Internet.

Likewise, evidence of a crime can be stored at a remote location, either for the purpose of concealing the crime from law enforcement and others, or simply because of the design of the network. In certain circumstances, the fact that the evidence is stored and held by a third party, such as an Internet service provider, might be helpful to law enforcement agencies who might be able to use lawful process to get that information. However, storing information remotely can also create a challenge to law enforcement, which cannot ignore the real-world limits of local, state, and national sovereignty and jurisdiction. Obtaining information from foreign countries, especially on an expedited basis, can be a daunting task, especially when a country may be in a different time zone, use a different language, have different legal rules, and may not have trained experts available. Consequently, even as the Internet and other new technologies have given us new abilities to find criminals remotely, our abilities can be hindered if we cannot obtain the necessary legal cooperation from our counterparts in other countries.

The vast majority of Internet companies are good corporate citizens and are interested in the safety of our citizens. In fact, several companies have been engaged in discussions with law enforcement regarding our concerns. Despite these efforts, we have learned that we cannot take for granted the nature of any Internet service provider's services, its record-keeping practices, and its ability or willingness to cooperate with us. We have encountered a handful of companies involved in criminal activity. In addition, even those companies that are not involved in criminal activities might not be able to assist us because of business reasons or privacy concerns that have resulted in them not keeping the records that will assist in the investigation of a particular crime.

Moreover, users connect to the Internet from anywhere in the world over old-fashioned telephone lines, wireless phones, cable modems, and satellite systems. Each of these telecommunications systems has its own protocols for addressing and routing traffic, which means that tracking all the way back to the criminal at his or her computer will require agents to be fluent in each technical language. Gathering this evidence from so many kinds of providers is a very different proposition from the days when we simply obtained an order for a telephone company to trace a threatening call.

Legal Challenges

Deterring and punishing computer criminals requires a legal structure that will support detection and successful prosecution of offenders. Yet the laws defining computer offenses, and the legal tools needed to investigate criminals using the Internet, can lag behind technological and social changes, creating legal challenges to law enforcement agencies.

We may be able to correct some of the legal challenges we encounter through legislative action. For example, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, arguably does not reach a computer hacker who causes a large amount of damage to a network of computers if no individual computer sustains over $5,000 worth of damage. The Department of Justice has encountered several instances in which intruders have gained unauthorized access to protected computers (whether publicly or privately owned) used in the provision of "critical infrastructure" systems and services—such as those that hospitals use to store sensitive information and to treat patients, and those that the military uses to defend the nation—but where proof of damage in excess of $5000 has not been readily available.

The laws under which we are able to identify the origin and destination of telephone calls and computer messages also need to be reviewed. For example, under current law we may have to obtain court orders in multiple jurisdictions to trace a single communication. Obtaining court orders in multiple jurisdictions does not advance any reasonable privacy safeguard, yet it can be a substantial impediment

to a fast-paced investigation. As the Attorney General testified recently, it might be extremely helpful, for instance, to provide nationwide effect for trap and trace orders.

Another concern focuses on the problem of online threats and serious harassment—that is, cyberstalking. Current Federal law does not address those situations where a cyberstalker uses unwitting third parties to bombard a victim with messages, transmits personal data about a person—such as the route by which the victim's children walk to school—in order to place such person or his family in fear of injury, or sends an e-mail or other communications under someone else's name with the intent to abuse, harass, or threaten that person. We believe Federal law may need to be amended to address this gap.

These aren't hypothetical changes that we are proposing to address. Just ask the California woman who was awakened six times in the middle of the night to find men knocking on her door offering to rape her. She discovered that a man whom she had told she was not romantically interested in had posted personal advertisements on a variety of Internet services pretending to be her. Each posting, which contained her home address and telephone number, claimed that she fantasized about being raped. We need to ensure that laws against harassment clearly prohibit such horrific actions, particularly since access to the Internet means immediate access to a wide audience.

While we believe changes in Federal law may be necessary to address these challenges, we also want to emphasize that any such legislation should be tailored to address the challenges we face and should avoid unnecessary infringement on personal privacy. We recognize the importance the public attaches to individual privacy, and any legislation must be carefully balanced to avoid unnecessary infringement on the privacy rights we hold dear in this country.

Resource Challenges

In addition to technical and legal challenges, we face significant resource challenges. Simply stated, we need an adequate number of prosecutors and agents—at the Federal, state and local level—trained with the necessary skills and properly equipped to effectively fight all types of cybercrime.

While Congress has been very supportive of the Department's cybercrime efforts, we need additional resources to ensure we are adequately equipped to continue our battle against cybercriminals. The President has requested $37 million in new money in FY 2001 to expand our staffing, training and technological capabilities to continue the fight against computer crime. Together, these enhancements will increase the Department's 2001 funding base for computer crime to $138 million, 28 percent more than in 2000.

Last, the Department of Justice would like to work with Congress to develop a comprehensive, five-year plan—with FY 2001 as our baseline—to prevent cybercrime and, when it does occur, to locate, identify, apprehend and bring to justice those responsible for these types of crimes. On February 16th, the Attorney General testified before Congress regarding a proposed a 10-point plan to identify the key areas we need to develop for our cybercrime capability. The key points of this plan she touched upon include:

- Developing a round-the-clock network of Federal, state and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cybercrime.
- Developing and sharing expertise—personnel and equipment—among Federal, state and local law enforcement agencies.
- Dramatically increasing our computer forensic capabilities, which are so essential in computer crime investigations—both hacking cases and cases where computers are used to facilitate other crimes, including drug trafficking, terrorism, and child pornography.
- Reviewing whether we have adequate legal tools to locate, identify, and prosecute cybercriminals. In particular, we may need new and more robust procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions. We also need to explore whether we have adequate tools at the Federal level to effectively investigate cybercrime.
- Because of the borderless nature of the Internet, we need to develop effective partnerships with other nations to encourage them to enact laws that adequately address cybercrime and to provide assistance in cybercrime investigations. A balanced international strategy for combating cybercrime should be at the top of our national security agenda.
- We need to work in partnership with industry to address cybercrime and security. This should not be a top-down approach through excessive Government

regulation or mandates. Rather, we need a true partnership, where we can discuss challenges and develop effective solutions that do not pose a threat to individual privacy.

- And we need to teach our young people about the responsible use of the Internet. The Department of Justice and the Information Technology Association of America have already taken steps to do so through the development of the Cybercitizen Partnership, but more needs to be done.

Efforts Against Cybercrime

Despite the technical, legal, and resource challenges, the Department has made strides in our fight against cybercrime. We have and will continue to develop extensive investigatory and prosecutorial programs to counter cybercrime. Let me take a few moments to details some of our efforts to date.

On the investigatory side, we have the FBI's National Infrastructure Protection Center (NIPC) and specialized squads located in 16 field offices.

On the prosecutorial side, we have trained attorneys, both in headquarters and in the field, who are experts in the legal, technological, and practical challenges involved in investigating and prosecuting cybercrime. The cornerstone of our prosecutor cybercrime program is the Computer Crime and Intellectual Property Section. CCIPS, which currently has 18 attorneys, was founded in 1991 as the Computer Crime Unit and was elevated to Section status in 1996. CCIPS works closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators" (CTC's) in U.S. Attorneys' Offices around the country. Each CTC is given special training and equipment, and serves as the district's expert in computer crime cases. As a result of these programs, the number of cases and prosecutions by the Department is growing at a tremendous rate. For example, in 1998, U.S. Attorneys' Offices filed 85 computer crime cases against 116 defendants. This represents a 29 percent increase in the number of cases filed and a 51 percent increase in the number of defendants, compared to the previous year. During that same period of time, a total of 62 cases against 72 defendants were terminated, with 78 percent of those defendants being convicted.

At the same time, our prosecutors are working with numerous other Federal, state, and local investigators and prosecutors, providing assistance in any case involving computers and other high technology, such as computer searches and seizure. In sum, the Department and, in particular, its investigators and prosecutors take seriously our responsibility to protect the nation's computers and the Internet from computer crime.

In addition to the Department's efforts, other agencies including the Customs Service, the Secret Service, the Securities and Exchange Commission, and the U.S. Postal Service's Inspectors General, have played a role in the investigation and prosecution of computer crimes.

Infrastructure Protection

The Department is also a full partner in ongoing efforts to assure our nation's critical infrastructures and to make them less vulnerable to the emerging risks of the information age.

I mentioned before that we believe strongly that *the private sector should take the lead in protecting private computer networks, through more vigilant security efforts, information sharing, and, where appropriate, cooperation with Government agencies.* Within this framework, and apart from prosecuting those who launch criminal attacks on our infrastructure (which is our critical responsibility), the Department can make important contributions. In the information sharing arena, we have continued some of the groundwork started by the President's Commission on Critical Infrastructure Protection by more closely examining the issues that may impede robust sharing of risk-related information between private sector entities, between Governmental entities, and between Government and the private sector.

As the private sector protects its networks, so must the Government. Therefore, the Department of Justice is working to ensure that its own networks are secure. We are also involved in efforts, under the auspices of the Critical Infrastructure Coordinating Group of the National Security Council, to help Federal agencies expedite and simplify the process of performing "vulnerability assessments," in order to uncover hidden vulnerabilities of critical Government systems before others try to do that for us.

Finally, the Justice Department also is involved in efforts to ensure that all programs arising out of the Federal Government's "infrastructure assurance" efforts are implemented in way entirely respects long-standing protections for the privacy rights of individuals.

Conclusion

On behalf of the Department of Justice, I want to thank Congress for all the support it has given to our efforts to combat cybercrimes. Advancements in technology indicate that our efforts are only just beginning. We look forward to working with Congress and the private sector to ensure that we have a robust and effective long-term plan for combating cybercrime, protecting our nation's infrastructure, safeguarding privacy, and ensuring that the Internet reaches its full potential for expanding communications, facilitating commerce, and bringing countless other benefits to our society.

Senator BURNS. Thank you very much, Mr. Holder. I appreciate that. Now we have Mr. William Reinsch, and Bill, thank you for coming back today. We have been across the table many times on different issues, and I appreciate your openness and your willingness to come down and visit with us on issues such as this. We are looking forward to your statement.

STATEMENT OF WILLIAM REINSCH, UNDER SECRETARY OF COMMERCE, BUREAU OF EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. REINSCH. Thank you, Mr. Chairman. It is always a pleasure to be here, particularly a pleasure to be here and not talk about encryption, so I am delighted to have the opportunity to have a different subject at hand.

My statement begins with some comments about the importance of computer networks and the Internet, and there is no committee that knows more about it than you all, so I think I will just get right into the meat of what I want to tell you this morning, Mr. Chairman.

Senator BURNS. Your complete statement will be made a part of the record, however, Mr. Secretary.

Mr. REINSCH. I appreciate that. Protecting our critical infrastructure requires that we draw on various assets of the Government. When specific incidents or cyber events occur, the Government needs the capacity to issue warnings, investigate the incident, and develop a case to punish the offenders. The National Information Protection Center at the FBI is organized to deal with such events as they occur. Over the long term, the Government also has a duty to be proactive to ensure that our computer systems are protected from attack.

Critical infrastructure protection involves assets of both the Government and the private sector. A number of agencies have responsibilities with respect to Government computer systems. The Department of Defense is well on its way to securing its critical systems, and OMB and NIST have responsibility for information resources management of computer systems in Federal agencies.

I want to make clear, Mr. Chairman, the Federal Government's responsibility in this area. The commission of crimes is only part of the equation. The infrastructures at risk are owned and operated by the private sector. The use of information technology is so embedded in the core operations and customer service delivery systems of industry that inevitably it will be they who must work together to take the steps necessary to protect themselves. However, we can help.

The first major step is the elevation of awareness across industry of the business case for action for leaders within industry. They

have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can also help identify problems, identify good practices and management practices and strategies, publicize them, encourage planning, promote research and development, and convene meetings, which is not a small matter.

In short, we can act as a catalyst for industry to mobilize. That is precisely the role the Commerce Department is playing in several ways. NTIA is a lead agency for the communications information sector. In February 1999, NTIA created a private sector coordinator consortium. The consortium is filled by representatives from the Information Technology Association of America, the Telecommunications Industry Association, and the U.S. Telecom Association, all groups I am sure you are familiar with.

Among their initiatives, the consortium has been raising awareness among industry through the exchange of information on threats and vulnerabilities, conducting information security surveys across sectors, and developing and assessing critical infrastructure-related standards and best practices. Perhaps our most important area right now is the development of what we are calling the Partnership for Critical Infrastructure Security. The partnership is a collaborative effort between industry and Government. It brings representatives of the infrastructure sector together in a dialog with each other and with other stakeholders, including the risk management and investment communities, mainstream businesses, and also State and local Governments.

Secretary Daley, Greg Rohde and I met with senior members of over 80 partnership companies in New York in December. We met again last month in Washington with over 220 senior members of more than 120 partnership companies to encourage business leaders to adopt information security as an integral business practice.

The partnership agreed to address such important issues as cross-sector vulnerability assessments, information-sharing, and R&D requirements. It set up working groups in those areas which are continuing to meet throughout the spring, and the next meeting of the full partnership will be this summer. The Department's Critical Infrastructure Assurance Office, or CIAO, also is assisting Federal agencies in conducting analyses of their dependencies on critical infrastructures.

CIAO has just finished an ambitious pilot program that identifies the critical assets of the Commerce Department and maps out dependencies on Governmental and private sector infrastructures. This program will provide important input to managers and security officials as they seek to assure their critical assets against cyber attacks. The Commerce Department through the CIAO also coordinated the development of the national plan for information systems protection. President Clinton announced the release of version 1.0 of the plan on January 7. This is it. If you do not have any, I would be pleased to provide you with thousands of them.

It represents the first attempt by any national Government to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and con-

trolled through the use of computers and computer networks. My full statement, Mr. Chairman, has substantial information about the details of the plan that I will pass over in the interest of time.

Finally, let me make a comment about funding. President Clinton has proposed increases for critical infrastructure protection substantially over the past 3 years, including a 15 percent increase in his fiscal year 2001 budget to $2.01 billion. He has also developed and funded new initiatives to defend the Nation's systems from cyber attack. For example, establishing a permanent export review team at NIST that will help agencies conduct vulnerability analyses and develop critical infrastructure protection plans, working to recruit, train, and retrain Federal information technology experts.

We have developed and provided fiscal year 2001 funding for a Federal cyber services training and education initiative led by OPM and the National Science Foundation, which calls for two programs. The first is an ROTC-like program, where we pay for information technology education in exchange for Federal service, and the second is a program to establish competencies and to certify our existing IT work force. As I think you, Mr. Chairman, or Senator Hollings commented that obtaining and retraining information technology workers in the Federal Government, whether it is in the law enforcement area or on the civilian side, is an extremely difficult thing to do.

We think this program will be an important first step, in addition to funding seven public key infrastructure model pilot programs in fiscal year 2001 at different Federal agencies, designing a Federal intrusion detection network, or FIDNET, to protect vital systems in Federal civilian agencies, and ensuring the rapid implementation of system patches for known software defects. FIDNET will operate in full compliance with all existing privacy laws.

Developing Federal R&D efforts. R&D investments in computer security will grow by 31 percent in the President's fiscal year 2001 budget. Part of that includes establishing an Institute for Information Infrastructure Protection in NIST, as recommended by the President's Committee of Advisors on Science and Technology, or PiCAST.

The institute would identify and address serious R&D gaps that neither the private sector nor the Government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President's 2001 budget provides $150 million for the institute.

Finally, the National Infrastructure Assurance Council, NIAC. The President signed an executive order creating this advisory council last year. Its members are now being recruited from the senior ranks of the critical infrastructure industries, including the information technology, State and local Governments, and we expect an announcement about that shortly.

In addition, the President has announced a number of new initiatives designed to support efforts for enhancing computer security, including the $9 million fiscal year 2000 budget supplemental that jump starts several of the key elements of next year's budget that I just mentioned.

In closing, Mr. Chairman, let me simply say that in early February Secretary Daley met with the President and 25 senior executives concerned about the recent disruptions to the Internet. This meeting reinforced the need for further cooperation between Government and industry to help the private sector to develop its action agenda for cyber security. The incidents of early February are not cause, in our judgment, for pushing the panic button, but they are a wake-up call for action.

As the President said, I think there is a way that we can clearly promote security. The President submitted a budget proposal that funds a number of initiatives that address critical information systems protection. If we are to reap the benefits of the information age, we need to take action to maintain public confidence in a secure business environment that ensures both our national security and the growth of our economy.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Reinsch follows:]

PREPARED STATEMENT OF WILLIAM REINSCH, UNDER SECRETARY OF COMMERCE, BUREAU OF EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. Chairman, I welcome this opportunity to appear before you to discuss the Federal Government's efforts to protect the nation's critical infrastructures.

Interdependent computer networks are an integral part of doing business in the Information Age. America is increasingly dependent upon computer networks for essential services, such as banking and finance, emergency services, delivery of water, electricity and gas, transportation, and voice and data communications. New ways of doing business in the 21st century are rapidly evolving. Business is increasingly relying on E-commerce for its commercial transactions as well as for its critical operations. At the same time, recent hacking attempts at some of the most popular commercial Web sites underscore that America's information infrastructure is an attractive target for deliberate attack or sabotage. These attacks can originate from a host of sources, such as terrorists, criminals, hostile nations, or the equivalent of car thief "joyriders." Regardless of the source, however, the potential for cyber damage to our national security and economy is evident.

Protecting our critical infrastructures requires that we draw on various assets of the Government. When specific incidents or cyber events occur, the Government needs a capacity to issue warnings, investigate the incident, and develop a case to punish the offenders. The National Information Protection Center at the FBI is organized to deal with such events as they occur.

Over the long term, the Government also has a duty to be proactive to ensure that our computer systems are protected from attack. Critical infrastructure protection involves assets of both the Government and the private sector. A number of agencies have responsibilities with respect to Government computer systems. The Department of Defense is well on its way to securing its critical systems, and the Office of Management and Budget (OMB) and the National Institute of Standards and Technology at the Department of Commerce (NIST) have responsibility for information resources management of computer systems in Federal agencies.

I want to make clear that the Federal Government's responsibility in this area with respect to the commission of crimes is only part of the equation. The infrastructures at risk are owned and operated by the private sector. The use of information technology is so embedded in the core operations and customer service delivery systems of industry that inevitably, it will be they who must work together to take the steps necessary to protect themselves. We can help. The first major step is the elevation of awareness across industry of the "business case for action" for leaders within industry. They have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can also help identify problems, good practices in management policies and strategies, and publicize them, encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst for industry to mobilize. That is precisely the role the Commerce Department is playing in several ways.

First, the National Telecommunications and Information Administration (NTIA) is lead agency for the communications and information sector. In February, 1999,

NTIA created a Private Sector Coordinator Consortium. This role is filled by representatives from the Information Technology Association of America (ITAA), the Telecommunications Industry Association (TIA), and the U.S. Telecom Association (USTA). Among their initiatives, the consortium has been raising awareness among industry through the exchange of information on threats and vulnerabilities, conducting information security surveys across sectors, and developing and asessing CIP-related standards and best practices.

Another active area is the development of the Partnership for Critical Infrastructure Security. The Partnership is a collaborative effort between industry and Government. This undertaking brings representatives of the infrastructure sectors together in a dialogue with each other and with other stakeholders, including the risk management and investment communities, mainstream businesses, and state and local Governments.

The Partnership complements the work of the Federal lead agencies responsible for working directly with the industry sectors in developing their critical infrastructure plans, including NTIA's work with the communications and information technology industries. It also complements the NIPC's focus on cyber-terrorism by encouraging industry to collaborate on information security issues.

Secretary Daley, Assistant Secretary for Communications and Information Gregory Rohde, and I met with senior members of over 80 Partnership companies in December in New York. We met again last month in Washington, D.C., with over 220 senior members of more than 120 Partnership companies to encourage business leaders to adopt information security as an integral business practice. The Partnership agreed to address such important issues as, cross-sector vulnerability assessments, information sharing, and R&D requirements.

The Commerce Department's Critical Infrastructure Assurance Office (CIAO) also is assisting Federal agencies in conducting analyses of their own dependencies on critical infrastructures. CIAO has just finished an ambitious pilot program that identifies the critical assets of the Commerce Department and maps out dependencies on Governmental and private sector infrastructures. This program will provide important input to managers and security officials as they seek to assure their critical assets against cyber attacks.

The Commerce Department, through the CIAO, coordinated the development of the *National Plan for Information Systems Protection.* President Clinton announced the release of Version 1.0 of the Plan on January 7.

It represents the first attempt by any national Government to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled through the use of computers and computer networks.

The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback. That is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a Dialogue*—to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.

II. The Plan: Overview and Highlights.

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes 10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

Program 1 calls for the Government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks from attack, and to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

Program 2 will install multi-layered protection on sensitive computer systems, including advanced fire walls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.

Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law. It will assist, transform, and strengthen U.S. law enforcement and intelligence agencies to be able to deal with a new kind of threat and a new kind of criminal—one that acts against computer networks.

Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner. This includes improving information sharing within the Federal Government and encouraging private industry, as well as, state and local Governments, to create Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local Governments, and could receive warning information from the Federal Government. Program 4 additionally calls for removal of existing legal barriers to information sharing.

Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and agency continuity and recovery plans the ability to deal with information attacks. The goal for Government and the recommendation for industry is that every critical information system have a recovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through.enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation's commitment to Prepare and Prevent and to Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that our information security technology stays abreast with changes in the threat environment.

Program 7 will survey the numbers of people and the skills required for information security specialists within the Federal Government and the private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-based attacks.

Program 9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation within the Federal Government, including Congress, and between the Government and private industry.

Program 10 builds mechanisms to highlight and address privacy issues in the development of each and every program. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties. The Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

With respect to funding, President Clinton has proposed increases for critical infrastructure protection substantially over the past three years, including a 15 percent increase in his FY 2001 budget to $2.01 billion. He has also developed and funded new initiatives to defend the nation's systems from cyber attack:

• Establishing a permanent Expert Review Team (ERT) at NIST that will help agencies conduct vulnerability analyses and develop critical infrastructure protection plans. ($5 million).
• Working to recruit, train, and retrain Federal IT Experts. We have developed and provided FY2001 funding for a Federal Cyber Services Training and Education initiative led by OPM and NSF which calls for two programs: the first is an ROTC-like program where we pay for IT education (B.S. or M.S.) in exchange for Federal service; and the second is a program to establish competencies and certify our existing IT workforce. ($25 million).
• Funding seven Public Key Infrastructure model pilot programs in FY 2001 at different Federal agencies. ($7 million).
• Designing a Federal Intrusion Detection Network (FIDNET) to protect vital systems in Federal civilian agencies, and in ensuring the rapid implementation of system "Apaches" for known software defects. FIDNET will operate in full compliance with all existing privacy laws. ($10 million).
• Developing Federal R&D Efforts. R&D investments in computer security will grow by 31 percent in the FY 2001 budget. ($606 million).
• Establishing an Institute for Information Infrastructure Protection. The Institute would identify and address serious R&D gaps that neither the private sector nor the Government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President's FY2001 budget provides funding of $50 million for the Institute. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this organization. The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and supported by leading corporate Chief Technology officers. ($50 million).
• National Infrastructure Assurance Council (NIAC). The President signed an Executive order creating this Advisory Council last year. Its members are now being recruited from senior ranks of the critical infrastructure industries, including the information technology, and state and local Governments.

In addition, the President announced a number of new initiatives designed to support efforts for enhancing computer security, including a $9 million FY 2000 budget supplemental to jump-start key elements of next year's budget.

In early February, Secretary Daley met with the President and 25 senior executives concerned about the recent disruptions to the Internet. This meeting reinforced the need for further cooperation between Government and industry to help the private sector develop its action agenda for cyber security. The incidents of early February are not cause for pushing the panic button, but they are a wake up call for action. As the President said, "I think there is a way that we can clearly promote security." The President has submitted a budget proposal that funds a number of initiatives that address critical information systems protection. If we are to reap the benefits of the Information Age, we need to take action to maintain public confidence in a secure business environment that ensures both our national security and the growth of our economy.

Senator BURNS. Thank you, Mr. Secretary. Now we hear from Mr. Michael Vatis, Deputy Assistant Director of the FBI here in Washington, D.C. It is nice to have you with us this morning.

STATEMENT OF MICHAEL A. VATIS, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, NATIONAL INFRASTRUCTURE PROTECTION PROGRAMS

Mr. VATIS. Thank you, Mr. Chairman, Senator Hollings and members of the Subcommittee. I want to thank you for inviting me here to discuss the growing problem of cybercrime and its impact on commerce. Our ability in law enforcement to deal with this growing crime problem will require the support of Congress, and I greatly appreciate your support, Mr. Chairman, and this Committee's support for the work that we have been about these last 2 years.

The recent denial of service attacks have thrust the security of our information infrastructure into the spotlight, but they are real-

ly only the most recent example of a large and growing problem of criminal activity in cyberspace. The cyber revolution has permeated many aspects, if not all aspects, of our lives, and we see its effects all around us, in the way we do business, in the way we communicate, and even in the way that Government agencies operate.

Unfortunately, that revolution has a downside, as you mentioned in your own statement, Mr. Chairman, and that downside is the effect that cyberspace and the new information technologies have on criminal activity, because criminals are increasingly seeing the utility of cyber tools both to facilitate traditional sorts of crimes like fraud schemes and extortion, and also to engage in new types of crimes, where computers and the information stored on them are seen as the targets of the criminal activity, rather than just facilitators of that activity.

Thus, we have seen criminals intruding into computers to steal credit cards, to steal money, to abscond with proprietary information, and to shut down e-commerce sites. And this is not just a crime problem. It is also a national security problem. That is because our Nation's critical infrastructures—including things such as telecommunications, electrical energy, and banking and finance, those things that are vital to our national security as well as our national economy—are all dependent on computer technology. But that very dependence makes them vulnerable to sorts of attacks that did not exist 10 or 15 years ago.

So the same basic types of cyber tools that are attractive now to criminals who are interested in illicit financial gain are also attractive to foreign intelligence services who might be seeking ways to obtain sensitive Government or private sector information, and also to terrorists or hostile foreign nations who are bent on attacking United States interests.

The difficulty of dealing with this challenge stems from the nature of the cyber environment itself. That environment is borderless. It affords easy anonymity and methods of concealment to bad actors, and it provides new tools that allow remote access to targeted computers. A criminal sitting on the other side of the planet is just as capable of stealthily infiltrating a computer network, or shutting an e-commerce site down, as is somebody sitting across the street from his target.

To deal with this problem in all its novel aspects, law enforcement must retool its work force, forge new partnerships with private industry and other agencies, and also work closely with our international counterparts, because so many of these events transcend national boundaries.

We have been doing all of these things for the last two years at the NIPC, but we must ensure that we can continue to build on our progress to ensure that we can protect the Nation's public safety and national security in the information age.

As you know, the NIPC is an interagency center located at the FBI, and we serve as a focal point for the Government's efforts, on the one hand, to warn of imminent or impending attacks, and also, on the other hand, to respond to any attacks that do occur. Regarding the number of our personnel, we have 94 authorized FBI positions at the NIPC, and we have 82 of those 94 people on board,

with the other dozen people in the pipeline and scheduled to come on board shortly.

We have a target of 40 detailees from other Government agencies—which is simply a target, since we are left, really, to the beneficence of other agencies to send people over to us to work with us, and we have got about half of our target on board, with some candidates in the pipeline as well that will come from those other agencies. But one of our challenges is to work with other agencies to get some people who have the right skills. Unfortunately there is a limited supply of those people in the Government, but we are working effectively with other agencies to ensure that they are represented at the Center, so we can build a good operational partnership.

We also have, in addition to the Center itself, an investigative program across the FBI field offices around the Nation, which consists of 193 special agents who are trained in conducting network investigations and who also engage in critical liaison with the private sector, and, very importantly, with State and local law enforcement, since they obviously must bear a large share of the load in dealing with this crime problem.

My written statement has a lengthy summary of examples of the many different types of cybercrime that we have dealt with over the last two years. I will mention here just two recent examples which I think point out the challenge and also the effects of cybercrime on e-commerce. Last Fall, we had the Melissa virus, which was a very quickly disseminating virus that affected numerous, customers and businesses. Within several days, working with AOL and the New Jersey State police, we were able to track down the propagator of that virus, and he recently pled guilty to both Federal and State charges. In his guilty plea, he admitted to affecting over a million computers and causing $80 million in damage from that one virus.

Then in February of this year, we had the distributed denial of service (DDOS) attacks on some of the most popular e-commerce sites, as the Deputy Attorney General mentioned. I, too, am limited in what I can say here about this pending investigation, but I can make a couple of points. First, even before the investigation, at the end of last year, when we had information that some of the malicious DDOS software was being implanted in universities and other private sector networks that would allow a hacker to take over those systems and use them to attack another target, we issued warnings to Government agencies and to the private sector so that people could take steps to see whether their own networks had been taken over without their knowledge, and so that they could remove any malicious code.

We also released a detection tool that we had created mainly for investigative uses, but which we also realized had possible utility for network protection. We made that tool available to private companies and Government agencies so that they could determine whether their networks had been taken over by a hacker.

Unfortunately, those efforts did not totally eliminate the threat, and at the beginning of last month we did see numerous sites being taken offline for several hours. As a result, we have initiated several investigations across the country. We have numerous special

agents following leads. We are also working very closely with several international counterparts to follow leads in their countries. Although I cannot go into detail, I can say we are making excellent progress. I am very satisfied with the progress we are making, and I am optimistic about the likelihood of having a successful resolution of at least some of these investigations.

Addressing the threat of cybercrime requires teamwork. That is the bottom line. We have to have good teamwork among Federal agencies, good teamwork between Federal and State and local law enforcement, and good teamwork between the Government and private sector.

We have developed partnerships with all of those other sectors over the last two years, and the one with the private sector is particularly important. Most of the victims of cybercrime are private companies, so successful investigation really depends on private companies letting us know when they have been victimized and working with us to provide us with incident information, and sometimes with technical assistance so that we can pursue investigations to the end.

The network administrator in a private company is oftentimes in many ways the lead investigator, because he or she is the one who really knows how his or her network is set up, and can lead an agent through the thicket of the network and come up with the important information that is necessary to an investigation.

I think the number of companies that have reported to us and have cooperated with us in the DDOS investigations is proof of the fact that private companies are realizing that they have to deal with law enforcement, and they are willing to engage in a good, cooperative venture with us. One of the keys to having a successful relationship with the private sector is for us to be able to demonstrate that we are capable of investigating these sorts of crimes. I think our track record over the last two years has shown that competence, and shown that we know how to investigate these cases, and our training efforts are enhancing our ability to do that.

We also need to show that we are willing to give information back to the private sector. We do not just want them to report to us. We are capable and willing to give them warnings when we have relevant information, and also to give them information about the nature of the threat and some of the technical exploits that we are seeing bad guys use. We have a number of programs that are geared toward sharing that information back to the private sector, which in turn is helping us to generate the confidence on the private sector's part that they can work with us.

I think it is a truism that commerce does not thrive in anarchy, and as Internet use soars, and e-commerce becomes a more significant part of our overall economy, it is in our national interest to ensure that the conditions exist that will foster the further growth of e-commerce. One of the conditions for that growth is enhancing the security of e-commerce sites so that customers can be confident that their privacy will be protected and that their credit cards will not be stolen, and so that businesses can be assured that they will not be knocked offline or robbed by cyber criminals.

Law enforcement has a significant role to play in fostering that security and ensuring that that confidence exists in cyberspace just

as in the physical world. It is important that we maintain and enhance our investigation capabilities to help establish that confidence and raise the level of security. We are only a part of the task, and the private sector bears the lion's share of the load in establishing better security on their own systems. But our role is a significant one, and we are very much tending to the business of ensuring that we can meet the challenge. I look forward to working with you, Mr. Chairman, and this Subcommittee to ensure that we continue to meet that threat.

Thank you very much.

[The prepared statement of Mr. Vatis follows:]

PREPARED STATEMENT OF MICHAEL A. VATIS, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, NATIONAL INFRASTRUCTURE PROTECTION PROGRAMS

Introduction

Mr. Chairman, Senator Hollings, and Members of the Subcommittee: Thank you for inviting me to discuss the threats to our Nation's critical infrastructures and the NIPC's approach to meeting those challenges. In 1998 the National Infrastructure Protection Center (NIPC) was established as a focal point for the Federal Government's efforts to protect the critical infrastructures. Much has happened since then to demonstrate both the wisdom of establishing such a Center and the seriousness of the problem it was designed to address. In the last two years we have seen the spread of destructive computer viruses affecting millions of users, a major international intrusion into Government computer networks, and denial-of-service attacks against some of the most popular e-commerce websites. Today I will focus on the nature of the national security and criminal threats we face in cyberspace, the progress we have made with our interagency partners in meeting those threats, and the continuing challenges we face.

The NIPC

The NIPC is an interagency Center located at the FBI. Created in 1998, the NIPC serves as the focal point for the Government's efforts to warn of and respond to cyber attacks, particularly those that are directed at our nation's "critical infrastructures." These infrastructures include telecommunications and information, energy, banking and finance, transportation, Government operations, and emergency services. In Presidential Decision Directive (PDD) 63, the President directed that the NIPC serve as a "national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." The PDD further states that the mission of the NIPC "will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response."

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

The Computer Investigations and Operations Section (CIOS) is the operational response arm of the Center. It supports and, where necessary, coordinates computer investigations conducted by FBI field offices and other agencies throughout the country, provides expert technical assistance to network investigations, and provides a cyber emergency response capability to coordinate the response to a national-level cyber incident.

The Analysis and Warning Section (AWS) serves as the "indications and warning" arm of the NIPC. It provides tactical analytical support during a cyber incident, and also develops strategic analyses of threats for dissemination to both Government and private sector entities so that they can take appropriate steps to protect themselves. Through its 24/7 watch and warning operation, it maintains a real-time situational awareness by reviewing numerous Governmental and "open" sources of information and by maintaining communications with partner entities in the Government and private sector. Through its efforts, the AWS strives to acquire indications of a possible attack, assess the information, and issue appropriate warnings to Government and private sector partners as quickly as possible

The Training, Outreach and Strategy Section (TOSS) coordinates the vital training of cyber investigators in the FBI field offices, other Federal agencies, and state and local law enforcement. It also coordinates outreach to private industry and Gov-

ernment agencies to build the partnerships that are key to both our investigative and our warning missions. In addition, this section manages our efforts to catalogue information about individual "key assets" across the country which, if successfully attacked, could have significant repercussions on our economy or national security. Finally, the TOSS handles the development of strategy and policy in conjunction with other agencies and the Congress.

Beyond the NIPC at FBI Headquarters, we have also created a cybercrime investigative program in all FBI Field Offices called the National Infrastructure Protection and Computer Intrusion (NIPCI) Program. This program, managed by the NIPC, consists of special agents in each FBI Field Office who are responsible for investigating computer intrusions, viruses, or denial of service attacks, for implementing our key asset initiative, and for conducting critical liaison activities with private industry. They are also developing cybercrime task forces in partnership with state and local law enforcement entities within their jurisdiction to leverage the limited resources in this area.

The Broad Spectrum of Threats

Over the past several years we have seen a wide range of cyber threats ranging from defacement of websites by juveniles to sophisticated intrusions that we suspect may be sponsored by foreign powers, and everything in between. Some of these are obviously more significant than others. The theft of national security information from a Government agency or the interruption of electrical power to a major metropolitan area would have greater consequences for national security, public safety, and the economy than the defacement of a web-site.

But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A web site hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce. Recent surveys confirm this point. According to a poll of Internet users by PC Data Online, 90 percent of those surveyed are concerned about the recent denial of service attacks. One in three surveyed said they were affected by the DDOS attacks. Further, over 40 percent of those surveyed said that they would be less likely to send credit card information over the Internet in the future.

Such surveys demonstrate the simple fact that the Internet has become a major aspect of everyday life for many Americans and is fast becoming a major part of our economy. There were over 100 million Internet users in the United States in 1999. That number is projected to reach 177 million in the United States and 502 million worldwide by the end of 2003. Electronic commerce has emerged as a new sector of the American economy, accounting for over $100 billion in sales during 1999, more than double the amount in 1998. By 2003, electronic commerce is projected to exceed $1 trillion. It should be no surprise, then, that as Internet use and e-commerce continue to grow at a rapid pace, the rate of cybercrime is also rising dramatically.

A significant part of the problem is the lack of adequate security on the Internet. As Lou Gerstner, the CEO of IBM said in a speech at Boston College on Monday, "No brick-and-mortar company would ever consider opening its doors without locks, video cameras and a security staff. Yet every day hundreds of Web enterprises do just that." A fundamental need, therefore, is to raise the level of security on the Internet. This is clearly the role of the private sector. The Government has neither the responsibility nor the expertise to act as the private sector's system administrator. We can help, however, by providing information to the private sector about concrete threats and the latest techniques being utilized by cyber criminals, so that private companies can take steps to secure their systems against those threats. We also need to ensure that law enforcement has the capabilities to investigate cybercrime that does occur.

The following are some of the categories of cyber threats that we confront today.

Insiders. The disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies. Insiders' knowledge of the target companies' network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The 1999 Computer Security Institute/FBI report notes that 55 percent of respondents reported malicious activity by insiders.

One example of an insider was George Parente. In 1997, Parente was arrested for causing five network servers at the publishing company Forbes, Inc., to crash. Parente was a former Forbes computer technician who had been terminated from

temporary employment. In what appears to have been a vengeful act against the company and his supervisors, Parente dialed into the Forbes computer system from his residence and gained access through a co-worker's log-in and password. Once online, he caused five of the eight Forbes computer network servers to crash, and erased all of the server volume on each of the affected servers. No data could be restored. Parente's sabotage resulted in a two day shut down in Forbes' New York operations with losses exceeding $100,000. Parente pleaded guilty to one count of violating of the Computer Fraud and Abuse Act, Title 18 U.S.C. 1030.

Hackers. Hackers (or "crackers") are also a common threat. They sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. The distributed denial-of-service (DDOS) attacks earlier this month are only the most recent illustration of the economic disruption that can be caused by tools now readily available on the Internet.

We have also seen a rise recently in politically motivated attacks on web pages or email servers, which some have dubbed "hacktivism." In these incidents, groups and individuals overload e-mail servers or deface web sites to send a political message. While these attacks generally have not altered operating systems or networks, they have disrupted services, caused monetary loss, and denied the public access to websites containing valuable information, thereby infringing on others' rights to disseminate and receive information.

Virus Transmitters. Virus transmitters are posing an increasingly serious threat to networks and systems worldwide. Last year saw the proliferation of several destructive computer viruses or "worms," including the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus. The NIPC frequently sends out warnings or advisories regarding particularly dangerous viruses, which can allow potential victims to take protective steps and minimize the destructive consequences of a virus.

The Melissa Macro Virus was a good example of our two-fold response—encompassing both warning and investigation—to a virus spreading in the networks. The NIPC sent out warnings as soon as it had solid information on the virus and its effects; these warnings helped alert the public and reduce the potential destructive impact of the virus. On the investigative side, the NIPC acted as a central point of contact for the field offices who worked leads on the case. A tip received by the New Jersey State Police from America Online, and their follow-up investigation with the FBI's Newark Division, led to the April 1, 1999 arrest of David L. Smith. Mr. Smith pleaded guilty to one count of violating 18 U.S.C. § 1030 in Federal Court, and to four state felony counts. As part of his guilty plea, Smith stipulated to affecting one million computer systems and causing $80 million in damage. Smith is awaiting sentencing.

Criminal Groups. We are also seeing the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. In September, 1999, two members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices (18 USC § 1029) and unauthorized access to a Federal interest computer (18 USC § 1030). The "Phonemasters" were an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the National Crime Information Center. Under judicially approved electronic surveillance orders, the FBI's Dallas Division made use of new data intercept technology to monitor the calling activity and modem pulses of one of the suspects, Calvin Cantrell. Mr. Cantrell downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual, who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Cantrell was sentenced to two years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

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

Another example of cyber intrusions used to implement a criminal conspiracy involved Vladimir L. Levin and numerous accomplices who illegally transferred more than $10 million in funds from three Citibank corporate customers to bank accounts in California, Finland, Germany, the Netherlands, Switzerland, and Israel between June and October 1994. Levin, a Russian computer expert, gained access over 40 times to Citibank's cash management system using a personal computer and stolen passwords and identification numbers. Russian telephone company employees working with Citibank were able to trace the source of the transfers to Levin's employer in St. Petersburg, Russia. Levin was arrested in March 1995 in London and subsequently extradited to the U.S. On February 24, 1998, he was sentenced to three years in prison and ordered to pay Citibank $240,000 in restitution. Four of Levin's accomplices pleaded guilty and one was arrested but could not be extradited. Citibank was able to recover all but $400,000 of the $10 million illegally transferred funds.

Unfortunately, cyberspace provides new tools not only for criminals, but for national security threats as well. These include terrorists, foreign intelligence agencies, and foreign militaries. Director of Central Intelligence George Tenet testified in February 2000, before the Senate Armed Services Committee, that many of the tools and weapons that can be used for information warfare purposes are "available on the open market at relatively little cost." The DCI went on to note that the critical threat of IW lies in its potential as a "force multiplier" for an adversary of the United States.

Three major categories of threat actors pose a national security challenge to the United States in cyberspace.

Terrorists. Terrorists groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. In his statement on the worldwide threat in 2000, Director of Central Intelligence George Tenet testified that terrorists groups, "including Hizbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qaeda organization are using computerized files, e-mail, and encryption to support their operations." In one example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. While we have not yet seen these groups employ cyber tools as a *weapon* to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. Moreover, we have seen other terrorist groups, such as the Internet Black Tigers (who are reportedly affiliated with the Tamil Tigers), engage in attacks on foreign Government web-sites and email servers. "Cyber terrorism"—by which I mean the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or Government operations) for the purpose of coercing or intimidating a Government or civilian population—is thus a very real, though still largely potential, threat.

Foreign intelligence services. Not surprisingly, foreign intelligence services have adapted to using cyber tools as part of their espionage tradecraft. Even as far back as 1986, before the worldwide surge in Internet use, the KGB employed West German hackers to access Department of Defense systems in the well-known "Cuckoo's Egg" case. While I cannot go into specifics about more recent developments in an open hearing, it should not surprise anyone to hear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. Government and private sector information.

Information Warfare. The prospect of "information warfare" by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional or "kinetic" weapons, nations see cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America's Achilles heel—our growing dependence on information technology in Government and commercial operations. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. And a Russian official has also commented that an attack on a critical infrastructure could, "by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."

Distributed Denial of Service Tools

The recent distributed denial of service (DDOS) attacks on e-commerce sites have garnered a tremendous amount of interest in the public and in the Congress. While we do not yet have official damage estimates, the Yankee Group, a research firm, estimates the impact of the attacks at $1.2 billion due to lost capitalization losses, lost revenues, and security upgrades. Because we are actively investigating these attacks, I cannot provide a detailed briefing on the status of our efforts. However, I can provide an overview of our activities to deal with the DDOS threat beginning last year and of our investigative efforts over the last three weeks. These attacks illustrate the growing availability of destructive, yet easy-to-use, exploits that are widely available on the Internet. They also demonstrate the NIPC's two-fold mission: sharing information with the private sector and warning of possible threats, and responding to actual attacks.

In the fall of last year, the NIPC began receiving reports about a new set of "exploits" or attack tools collectively called distributed denial of service (or DDOS) tools. DDOS variants include tools known as "Trin00," "Tribal Flood Net" (TFN), "TFN2K," and "Stacheldraht" (German for "barbed wire"). These tools essentially work as follows: hackers gain unauthorized access to a computer system(s) and place software code on it that renders that system a "master" (or a "handler"). The hackers also intrude into other networks and place malicious code which makes those systems into agents (also known as "zombies" or "daemons" or "slaves"). Each Master is capable of controlling multiple agents. In both cases, the network owners normally are not aware that dangerous tools have been placed and reside on their systems, thus becoming third-party victims to the intended crime.

The "Masters" are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents, activating their DDOS ability. The agents then generate numerous requests to connect with the attack's ultimate target(s), typically using a fictitious or "spoofed" IP (Internet Protocol) address, thus providing a falsified identity as to the source of the request. The agents act in unison to generate a high volume of traffic from several sources. This type of attack is referred to as a SYN flood, as the SYN is the initial effort by the sending computer to make a connection with the destination computer. Due to the volume of SYN requests the destination computer becomes overwhelmed in its efforts to acknowledge and complete a transaction with the sending computers, degrading or denying its ability to complete service with legitimate customers—hence the term "Denial of Service". These attacks are especially damaging when they are coordinated from multiple sites—hence the term Distributed Denial of Service.

An analogy would be if someone launched an automated program to have hundreds of phone calls placed to the Capitol switchboard at the same time. All of the good efforts of the staff would be overcome. Many callers would receive busy signals due to the high volume of telephone traffic.

In November and December, the NIPC received reports that universities and others were detecting the presence of hundreds of agents on their networks. The number of agents detected clearly could have been only a small subset of the total number of agents actually deployed. In addition, we were concerned that some malicious actors might choose to launch a DDOS attack around New Year's Eve in order to cause disruption and gain notoriety due to the great deal of attention that was being payed to the Y2K rollover. Accordingly, we decided to issue a series of alerts in December to Government agencies, industry, and the public about the DDOS threat.

Moreover, in late December, we determined that a detection tool that we had developed for investigative purposes might also be used by network operators to detect the presence of DDOS agents or masters on their operating systems, and thus would enable them to remove an agent or master and prevent the network from being unwittingly utilized in a DDOS attack. Moreover, at that time there was, to our knowledge, no similar detection tool available commercially. We therefore decided to take the unusual step of releasing the tool to the Department of Defense, other Government agencies, and to the public in an effort to reduce the level of the threat. We made the first variant of our software available on the NIPC web site on December 30, 1999. To maximize the public awareness of this tool, we announced its availability in an FBI press release that same date. Since the first posting of the tool, we have posted three updated versions that have perfected the software and made it applicable to different operating systems.

The public has downloaded these tools tens of thousands of times from the web site, and has responded by reporting many installations of the DDOS software, thereby preventing their networks from being used in attacks and leading to the opening of criminal investigations both before and after the widely publicized at-

tacks of the last few weeks. Our work with private companies has been so well received that the trade group SANS awarded their yearly Security Technology Leadership Award to members of the NIPC's Special Technologies Applications Unit.

Last month, we received reports that a new variation of DDOS tools was being found on Windows operating systems. One victim entity provided us with the object code to the tool found on its network. On February 18 we made the binaries available to anti-virus companies (through an industry association) and the Computer Emergency Response Team (CERT) at Carnegie Mellon University for analysis and so that commercial vendors could create or adjust their products to detect the new DDOS variant. Given the attention that DDOS tools have received in recent weeks, there are now numerous detection and security products to address this threat, so we determined that we could be most helpful by giving them the necessary code rather than deploying a detection tool ourselves.

Unfortunately, the warnings that we and others in the security community had issued about DDOS tools last year, while alerting many potential victims and reducing the threat, did not eliminate the threat. Quite frequently, even when a threat is known and patches or detection tools are available, network operators either remain unaware of the problem or fail to take necessary protective steps. In addition, in the cyber equivalent of an arms race, exploits evolve as hackers design variations to evade or overcome detection software and filters. Even security-conscious companies that put in place all available security measures therefore are not invulnerable. And, particularly with DDOS tools, one organization might be the victim of a successful attack despite its best efforts, because another organization failed to take steps to keep itself from being made the unwitting participant in an attack.

On February 7, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. Still, the challenges to apprehending the suspects are substantial. In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

The resources required in an investigation of this type are substantial. Companies have been victimized or used as "hop sites" in numerous places across the country, meaning that we must deploy special agents nationwide to work leads. We currently have seven FBI field offices with cases opened and all the remaining offices are supporting the offices that have opened cases. Agents from these offices are following up literally hundreds of leads. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers (ISPs), and providing all-source analytical assistance to field offices. Moreover, parts of the evidentiary trail have led overseas, requiring us to work with our foreign counterparts in several countries through our Legal Attaches (Legats) in U.S. embassies.

While the crime may be high tech, investigating it involves a substantial amount of traditional investigative work as well as highly technical work. Interviews of network operators and confidential sources can provide very useful information, which leads to still more interviews and leads to follow-up. And victim sites and ISPs provide an enormous amount of log information that needs to be processed and analyzed by human analysts.

Despite these challenges, I am optimistic that the hard work of our agents, analysts, and computer scientists; the excellent cooperation and collaboration we have with private industry and universities; and the teamwork we are engaged in with foreign partners will in the end prove successful.

Interagency Cooperation

The broad spectrum of cyber threats described earlier, ranging from hacking to foreign espionage and information warfare, requires not just new technologies and skills on the part of investigators, but new organizational constructs as well. In most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of his attack—i.e., whether an intrusion is isolated or part of a broader pattern affecting numerous targets. This means it is often impossible to determine at the outset if an intrusion is an act of cyber vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from the victim sites and intermediate sites such as ISPs and telecommunications carriers. Under

our constitutional system, such information typically can be gathered only pursuant to criminal investigative authorities. This is why the NIPC is part of the FBI, allowing us to utilize the FBI's legal authorities to gather and retain information and to act on it, consistent with constitutional and statutory requirements.

But the dimension and varied nature of the threats also means that this is an issue that concerns not just the FBI and law enforcement agencies, but also the Department of Defense, the Intelligence Community, and civilian agencies with infrastructure-focused responsibility such as the Departments of Energy and Transportation. It also is a matter that greatly affects state and local law enforcement. This is why the NIPC is an interagency center, with representatives detailed to the FBI from numerous Federal agencies and representation from state and local law enforcement as well. These representatives operate under the direction and authority of the FBI, but bring with them expertise and skills from their respective home agencies that enable better coordination and cooperation among all relevant agencies, consistent with applicable laws.

We have had many instances in the last two years where this interagency cooperation has proven critical. As mentioned earlier, the case of the Melissa virus was successfully resolved with the first successful Federal prosecution of a virus propagator in over a decade because of close teamwork between the NIPCI squad in the FBI's Newark Division and other field offices, the New Jersey State Police, and the NIPC.

The "Solar Sunrise" case is another example of close teamwork with other agencies. In 1998, computer intrusions into U.S. military computer systems occurred during the Iraq weapons inspection crisis. Hackers exploited known vulnerabilities in Sun Solaris operating systems. Some of the intrusions appeared to be coming from the Middle East. The timing, nature, and apparent source of some of the attacks raised concerns in the Pentagon that this could be a concerted effort by Iraq to interfere with U.S. troop deployments. NIPC coordinated a multi-agency investigation which included the FBI, the Air Force Office of Special Investigations, the National Aeronautics and Space Administration, the Department of Justice, the Defense Information Systems Agency, the National Security Agency, and the Central Intelligence Agency. Within several days, the investigation determined that the intrusions were not the work of Iraq, but of several teenagers in the U.S. and Israel. Two juveniles in California pleaded guilty to the intrusions, and several Israelis still await trial. The leader of the Israeli group, Ehud Tenenbaum, has been indicted and is currently scheduled for trial in Israel in April.

More recently, we observed a series of intrusions into numerous Department of Defense and other Federal Government computer networks and private sector entities. Investigation last year determined that the intrusions appear to have originated in Russia. The intruder successfully accessed U.S. Government networks and took large amounts of unclassified but sensitive information, including defense technical research information. The NIPC coordinated a multi-agency investigation, working closely with FBI field offices, the Department of Defense, and the Intelligence Community. While I cannot go into more detail about this case here, it demonstrates the very real threat we face in the cyber realm, and the need for good teamwork and coordination among Government agencies responsible for responding to the threat.

Private Sector Cooperation

Our success in battling cybercrime also depends on close cooperation with private industry. This is the case for several reasons. First, most of the victims of cybercrimes are private companies. Therefore, successful investigation and prosecution of cybercrimes depends on private victims reporting incidents to law enforcement and cooperating with the investigators. Contrary to press statements by cyber security companies that private companies won't share information with law enforcement, many private companies have reported incidents and threats to the NIPC or FBI field offices. The number of victims who have voluntarily reported DDOS attacks to us over the last few weeks is ample proof of this. While there are undoubtedly companies that would prefer not to report a crime because of fear of public embarrassment over a security lapse, the situation has improved markedly. Companies increasingly realize that deterrence of crime depends on effective law enforcement, and that the long-term interests of industry depend on establishing a good working relationship with Government to prevent and investigate crime.

Testimony two weeks ago before the Senate Appropriations Subcommittee for Commerce, State, and Justice by Robert Chesnut, Associate General Counsel for eBay, illustrates this point:

> Prior to last week's attacks, eBay had established a close working relationship with the computer crimes squad within the Northern California office of the Federal Bureau of Investigation ("FBI"). eBay has long recognized that the best way to combat cybercrime, whether it's fraud or hacking, is by working cooperatively with law enforcement. Therefore, last year we established procedures for notifying the FBI in the event of such an attack on our web site. As result of this preparation, we were able to contact the FBI computer intrusion squad during the attack and provide them with information that we expect will assist in their investigation. In the aftermath of the attack, eBay has also been able to provide the FBI with additional leads that have come to our attention.

Second, the network administrator at a victim company or ISP is critical to the success of an investigation. Only that administrator knows the unique configuration of her system, and she typically must work with an investigator to find critical transactional data that will yield evidence of a criminal's activity.

Third, the private sector has the technical expertise that is often critical to resolving an investigation. It would be impossible for us to retain experts in every possible operating system or network configuration, so private sector assistance is critical. In addition, many investigations require the development of unique technical tools to deal with novel problems. Private sector assistance has been critical there as well.

We have several other initiatives devoted to private sector outreach that bear mentioning here. The first is called "InfraGard." This is an initiative that we have developed in concert with private companies and academia to encourage information-sharing about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats. A vital component of InfraGard is the ability of industry to provide information on intrusions to the local FBI field office using secure e-mail communications in both a "sanitized" and detailed format. The local FBI field offices can, if appropriate, use the detailed version to initiate an investigation; while NIPC Headquarters can analyze that information in conjunction with other information we obtain to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. The key to this system is that whether, and what, to report is entirely up to the reporting company. A secure web site also contains a variety of analytic and warning products that we make available to the InfraGard community. The success of InfraGard is premised on the notion that sharing is a two-way street: the NIPC will provide threat information that companies can use to protect their systems, while companies will provide incident information that can be used to initiate an investigation and to warn other companies.

Our Key Asset Initiative (KAI) is focused more specifically on the owners and operators of critical components of each of the infrastructure sectors. It facilitates response to threats and incidents by building liaison and communication links with the owners and operators of individual companies and enabling contingency planning. The KAI began in the 1980s and focused on physical vulnerabilities to terrorism. Under the NIPC, the KAI has been reinvigorated and expanded to focus on cyber vulnerabilities as well. The KAI currently involves determining which assets are key within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets. FBI field offices are responsible for developing a list of the assets within their respective jurisdictions, while the NIPC maintains the national database. The KAI is being developed in coordination with DOD and other agencies. Currently the database has about 2600 entries. This represents 2600 contacts with key private sector nodes made by the NIPC and FBI field offices.

A third initiative is a pilot program we have begun with the North American Electrical Reliability Council (NERC). Under the pilot program, electric utility companies and other power entities transmit cyber incident reports in near real time to the NIPC. These reports are analyzed and assessed to determine whether an NIPC warning, alert, or advisory is warranted. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC *back* to the power companies fully justify their participation in the program. It is our expectation that the Electrical Power Indications and Warning System will provide a full-fledged model for the other critical infrastructures.

Much has been said over the last few years about the importance of information sharing. Since our founding, the NIPC has been actively engaged in building con-

crete mechanisms and initiatives to make this sharing a reality, and we have built up a track record of actually sharing useful information. These efforts belie the notions that private industry won't share with law enforcement in this area, or that the Government won't provide meaningful threat data to industry. As companies continue to gain experience in dealing with the NIPC and FBI field offices, as we continue to provide them with important and useful threat information, and as companies recognize that cybercrime requires a joint effort by industry and Government together, we will continue to make real progress in this area.

Meeting the Growing Cyber Threat

As Internet use continues to soar, the number of cyber attacks is also increasing exponentially. Our case load reflects this growth. In FY 1998, we opened 547 computer intrusion cases; in FY 1999, that number jumped to 1154. Similarly, the number of pending cases increased from 206 at the end of FY 1997, to 601 at the end of FY 1998, to 834 at the end of FY 99, and to over 900 currently. These statistics include only computer intrusion cases, and do not account for computer facilitated crimes such as Internet fraud, child pornography, or e-mail extortion efforts. In these cases, the NIPC and NIPCI squads often provide technical assistance to traditional investigative programs responsible for these categories of crime.

We can clearly expect these upward trends to continue, and for the threats to become more serious. While insiders, hackers, and criminal groups make up much of our case load at the moment, we can anticipate a growing number of national security cases in the near future. To meet this challenge, we must ensure that we have adequate resources, including both personnel and equipment, both at the NIPC and in FBI field offices. We currently have 193 agents nationwide dedicated to investigating computer intrusion and virus cases. In order to maximize investigative resources the FBI has taken the approach of creating regional squads in 16 field offices that have sufficient size to work complex intrusion cases and to assist those field offices without a NIPCI squad. In those field offices without squads, the FBI is building a baseline capability by having one or two agents to work NIPC matters, i.e. computer intrusions (criminal and national security), viruses, InfraGard, state and local liaison, etc.

At the NIPC, we currently have 101 personnel on board, including 82 FBI employees and 19 detailees from other Government agencies. This cadre of investigators, computer scientists, and analysts perform the numerous and complex tasks outlined above, and provide critical coordination and support to field office investigations. As the crime problem grows, we need to make sure that we keep pace by bringing on board additional personnel, including from other agencies and the private sector.

In addition to putting in place the requisite number of agents, analysts, and computer scientists in the NIPC and in FBI field offices, we must fill those positions by recruiting and retaining personnel who have the appropriate technical, analytical, and investigative skills. This includes personnel who can read and analyze complex log files, perform all-source analysis to look for correlations between events or attack signatures and glean indications of a threat, develop technical tools to address the constantly changing technological environment, and conduct complex network investigations. There is a very tight market for information technology professionals. The Federal Government needs to be able to recruit the very best people into its programs. Fortunately, we can offer exciting, cutting-edge work in this area and can offer agents, analysts, and computer scientists the opportunities to work on issues that no one else addresses, and to make a difference to our national security and public safety. In addition, Congress provided the FBI with a pilot program that exempts certain technical personnel from the Title V civil service rules, which allows us to pay more competitive salaries and recruit and retain top notch personnel. Unfortunately, this pilot is scheduled to expire in November unless extended.

Training and continuing education are also critical, and we have made this a top priority at the NIPC. In FY 1999, we trained 383 FBI and other-Government-agency students in NIPC sponsored training classes on network investigations and infrastructure protection. The emphasis for 2000 is on continuing to train Federal personnel while expanding training opportunities for state and local law enforcement personnel. During FY 2000, we plan to train approximately 740 personnel from the FBI, other Federal agencies, and state and local law enforcement.

Developing and deploying the best equipment in support of the mission is also very important. Not only do investigators and analysts need the best equipment to conduct investigations in the rapidly evolving cyber system but the NIPC must be on the cutting edge of cyber research and development. Conducting a network intrusion or denial-of-service investigation often requires analysis of voluminous amounts of data. For example, one network intrusion case involving an espionage matter currently being investigated has required the analysis of 17.5 Terabytes of data. To

place this into perspective, the entire collection of the Library of Congress, if digitized, would comprise only 10 Terabytes. The Yahoo DDOS attack involved approximately 630 Gigabytes of data, which is equivalent to enough printed pages to fill 630 pickup trucks with paper. Technical analysis requires high capacity equipment to store, process, analyze, and display data. Again, as the crime problem grows, we must ensure that our technical capacity keeps pace. We are also working closely with other agencies to ensure that we leverage existing resources to the fullest extent possible.

Challenges in Combating Cyber Intrusions

The burgeoning problem of cyber intrusions, viruses, and denial of service attacks poses unique challenges to the NIPC. These challenges require novel solutions, close teamwork among agencies and with the private sector, and adequate human and technical resources.

Identifying the Intruder. One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking your system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. The "Solar Sunrise" case illustrates this point. This will continue to pose a problem as long as the Internet remains rife with vulnerabilities and allows easy anonymity and concealment.

Jurisdictional Issues. Another significant challenge we face is intrusions involving multiple jurisdictions. A typical investigation involves victim sites in multiple states and often many countries. This is the case even when the hacker and victim are both located in the United States. In the United States, we can subpoena records, engage in judicially approved electronic surveillance, and execute search warrants on suspects' homes, seize evidence, and examine it. We can do none of those things ourselves overseas; rather, we depend on the local authorities to assist us. In some cases the local police forces simply do not understand or cannot cope with the technology. In other cases, these nations simply do not have laws against computer intrusions and are therefore limited in their ability to help us. FBI Legal Attaches in 35 embassies abroad provide critical help in building bridges with local law enforcement to enhance cooperation on cybercrime and in working leads on investigations. As the Internet spreads to even more countries, we will see greater demands placed on the Legats to support computer crime investigations. The NIPC also has held international computer crime conferences and offered cybercrime training classes to foreign law enforcement officials to develop liaison contacts and bring these officials up to speed on cybercrime issues.

The most difficult situation will arise, however, in which a foreign country with interests adverse to our own simply refuses to cooperate. In such a situation, we could find that an investigation is stymied unless we find an alternative method of tracing the activity back to its source.

The Role of Law Enforcement

Finally, I would like to conclude by emphasizing two key points. The first is that our role in combating cybercrime is essentially two-fold: (1) preventing cyber attacks before they occur or limiting their scope by disseminating warnings and advisories about threats so that potential victims can protect themselves; and (2) responding to attacks that do occur by investigating and identifying the perpetrator. This is very much an operational role. Our role is **not** to determine what security measures private industry should take, or to ensure that companies or individuals take them. It is the responsibility of industry to ensure that appropriate security tools are made available and are implemented. We certainly can assist industry by alerting them to the actual threats that they need to be concerned about, and by providing information about the exploits that we are seeing criminals use. But network administrators, whether in the private sector or in Government, are the first line of defense.

Second, in gathering information as part of our warning and response missions, we rigorously adhere to constitutional and statutory requirements. Our conduct is strictly limited by the Fourth Amendment, statutes such as Title III and ECPA, and the Attorney General Guidelines. These rules are founded first and foremost on the protection of privacy inherent in our constitutional system. Respect for privacy is thus a fundamental guidepost in all of our activities.

Conclusion

I want to thank the Subcommittee again for giving me the opportunity to testify here today. The cyber threat is real, multifarious, and growing. The NIPC is moving aggressively to meet this challenge by training investigators and analysts to investigate computer intrusion cases, equipping them with the latest technology, developing our analytic capabilities and warning mechanisms to head off or mitigate attacks, and closely cooperating with the private sector. We have already made considerable progress in developing our capabilities to protect public safety and national security in the Information Age. I look forward to working with Congress to ensure that we continue to be able to meet the threat as it evolves and grows. Thank you.

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

We have been joined by Senator Wyden. Do you have a statement, Senator?

Senator WYDEN. Thank you, Senator. I will just wait for questions.

Senator BURNS. Thank you.

I want to preface my line of thinking here just a little bit. We have an economic thing that is happening right now in the American business world, and in fact our whole economics, and we have this terrific increase in energy prices, which is going to create a little more pressure, I think, on the Internet, the way we move information, the way we do business, because of the cost of transportation to be right honest with you.

I think before the summer is out you are going to see we are going to be in a crisis situation. I cannot imagine right now my farmers, and this is a long way from what we are talking about, but I cannot imagine doubling the cost of fuel and trying to sell a product off the farm now that is not making any money under the conditions of last year, and now we are going to double our input cost and expect the same price this year.

I cannot imagine me even cranking the first flywheel on a tractor, to be right honest with you, but we have that moving, and I have a feeling this is going not only in the way we move information but also our e-commerce is going to have new pressures, as far as volume is concerned, in the upcoming year as we face this energy situation for the rest of the year, so I want to preface that, and that is what I am kind of concerned about.

Then we talk about security. Mr. Holder, with the exception to formal hearings, have you been in any communications with any of the Members of Congress regarding this situation to describe to them what your concerns are and the needs we are going to have?

Now, the representative from the Federal Bureau of Investigation says it is going to take a lot of teamwork between industry, Government, between Government agencies within the Government, and I am saying that I do not think I have had one call from one agency saying we have got a phenomenon out here that is working and some way or another we are going to have to deal with this.

And Congress I think will play a role and has to play a role in the future, but have you had any kind of meetings with Congress to bring us, Senator Hollings or whoever, up to date on the role that we should be playing, and especially your concerns about security and these kinds of situations?

Mr. HOLDER. To my knowledge there has been work, I think, at the staff level. I have not convened any meetings with any Mem-

bers of Congress, but I think we have had meetings at the staff level to talk about the needs we have identified both with regard to legislation and resources.

The Attorney General has talked about the creation of a 5-year plan starting in the next fiscal year to figure out exactly what challenges we think we are going to face, what resources we think we are going to need to face those challenges, and we think in that regard, in the formulation of that plan in particular, that interaction with Congress on the Senate side and the House side would be particularly important.

Senator BURNS. I say that because sometimes in these situations we are kind of behind the curve, even though you may have some facts that maybe we can prevent—and I am not saying that we have got the answers, but I am saying, though, that Congress finally has to play a role somewhere along the line in consultation between the agencies and Congress.

It would certainly help us, some of us—and even on the security side, can you give me, any of you can give me a profile of what kind of personalities engage in these destructive and senseless attacks like we have experienced?

Mr. VATIS. I am actually reluctant to state any one profile because there is a tremendous range of different types of actors that we see, ranging from the insider, an employee or a former employee at a company who wants to take revenge against his employer and so steals information to give to a competitor, or shuts down the system just to spite his employer. Teenage hackers who are breaking into systems just for bragging rights in the hacker community, or for the challenge of doing it.

More and more, organized groups of often young people but not necessarily juveniles who are breaking into systems to steal things for financial gain, and then all the way on the other end of the spectrum, foreign intelligence services that we are seeing looking at these new tools as a new mechanism for gathering information, so it really runs the gamut across that broad range.

Senator BURNS. Senator Hollings.

Senator HOLLINGS. I am encouraged by the appearance of each of you, and particularly Mr. Vatis, that the FBI is on top of it. We have had the Appropriations Committee hearings on this, and topic currently, under Senator Gregg's leadership we have been getting into child pornography and other internet-related issues.

The grasp of these subjects is necessary, but I would dissent from the idea expressed, and the timidity, about how the private sector should do this. Look here, if the private sector could do it they would find money in it and do it.

We got into the Internet to secure our communications. We said back in the late sixties, suppose they drop a bomb on the Pentagon and we have got all the troops out there—divisions and tanks and planes—but nobody can communicate. So then we started tying together research endeavors on the various university campuses, and ergo, the Internet. Now it is our responsibility of the infrastructure to get the security.

I have got to go, Mr. Chairman, right down to the conference on the FAA authorization bill. Before I go, let me note that we have to make sure that our transportation systems line air transpor-

tation are secure. You would not want somebody to muck up the radar and everything else at Reagan National and suddenly have the planes start crashing all around. None of us wants to go to an interview and say, "well, you know, we just had a hearing on it, and we all agreed it is the private sector's responsibility. Let the planes crash." I mean, come on.

Let's get away from this argument that security is a private sector responsibility. After all this industry is developing pell-mell into oligopolies where two or three more or less control the market and whereby no one else can get in.

We find Microsoft, for example, buying up some 200 different individual little endeavors, anytime anybody comes in with a new idea, the oligopoly comes in and says, whoopee, we will pay you so much or we will extinguish it. So you take the money, and that ends that.

The Government has a fundamental role in the Internet. Let's stop waiting on the partnerships and let's face our responsibility to secure our own infrastructure. We need to protect our own departments, communications, power, transportation, and otherwise. Can we do it? Is it possible? Who can answer that? Can we really make it secure, do you think?

Mr. VATIS. I will just briefly address that. I think we absolutely can. I think the technology exists, and is being developed, to secure our systems. I think there has been a rush to market with new features for competitive reasons, and security has lagged behind as a concern of the manufacturers.

Senator HOLLINGS. What you are telling me, and you can interrupt me, is if I can make it secure, then I can certainly guarantee the privacy, because I can make certain that that security is not invaded, is that right, and logical?

Mr. VATIS. I think the means exist to protect privacy, to protect the operability of systems, and I think we are seeing some significant strides in that direction.

I think I agree with you that the Federal Government does have primary responsibility, certainly for securing its own systems, and certainly for carrying out law enforcement responsibilities. which is a fundamental task of Government, and for issuing warnings about attacks.

But the one place I think that the private sector does have the primary responsibility is for ensuring its own security. If a business goes into e-commerce and puts out a Web site through which it transacts business with customers, it cannot be our responsibility in the Government to tell them how to secure that system, or to regulate how they do that. That is what I mean by security being primarily the private sector's responsibility.

Senator HOLLINGS. At DARPA, we gave all our research technology over to Boeing and Lockheed, and they are going like gangbusters. There is a similar situation at the National Institute of Standards and Technology. We farm out all of that technology. We are not trying to hold it, but we are trying to find it.

It is very interesting, Mr. Chairman, because your bill got this gentleman, Mr. Reinsch—it is interesting that he is from the Export Administration. He is not from any security—he is not from any technology. He is from exports, and here he appears from the

Export Administration. Now, correct me, and tell me about your technology.

Mr. REINSCH. What my bureau does, Senator Hollings, is control the export of critical technology products for national security reasons.

Senator HOLLINGS. That is how you got in it, and that is the only reason that we woke up here, at the congressional level, because of the export of the technology. It was not because of the import, the use, the development, the securing, or the infrastructure of the U.S. Government.

Mr. REINSCH. Well, if I could comment on several of your points, that part I think has proven to be an area of much broader agreement, and typically in a debate environment, there is less attention paid to it. If you will look at the plan, you will find most of it and most of the Government's resources right now, in fact, are devoted to precisely what you are talking about, which is the protection of Federal Government critical systems and assets.

Senator HOLLINGS. Is there any need otherwise in what you have outlined? I like the President's plan, but you know from experience you have got all the resources. You are heading it up. Do you need any help, and do we need to pass any law or fund any policy that you can think of?

Mr. REINSCH. Let me say tactfully, Senator Hollings, that the Appropriations Committees have been very generous to law enforcement and national security, and less generous to the Commerce Department and civilian agencies that have some of these same responsibilities.

Senator HOLLINGS. How much more do you need at the Commerce Department?

Mr. REINSCH. Well, we support the President's request, for 2001.

Senator HOLLINGS. How about your request? What else would you like to have?

Mr. REINSCH. For my particular bureau? You do not want me to start on that.

[Laughter.]

Senator HOLLINGS. In all fairness, tell us what you need to do the job.

Mr. REINSCH. For this function, we have requested and could use actually sooner than next year an additional $3½ million, which is peanuts compared to the whole thing.

Senator HOLLINGS. I worry about it, because you three have got a grasp on exactly what my concern is, that the Government gets in here and gets on top of infrastructure security that these functions are properly funded and properly coordinated. From your presentations here this morning, the coordination seems to be there, but it is a mammoth task. If industry could do it, they would have already done it and sold it, you know what I mean?

Thank you very much, Mr. Chairman.

Mr. REINSCH. There are areas, Mr. Chairman, if I could comment, where we think industry is not going to do it, frankly, because there is not any money in it.

Senator HOLLINGS. Thank you. We have had a hearing.

[Laughter.]

Mr. REINSCH. That is the genesis in part of the NIST request for its institute.

Senator Hollings.

Senator BURNS. Is the hearing over?

[Laughter.]

Senator HOLLINGS. No. We finally got what we wanted.

Senator BURNS. Senator Wyden.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you, Mr. Chairman. A couple of questions for you if I could, Mr. Holder. My judgment is that the challenge here is more one of enforcement of existing law, rather than trying to develop a whole lot of new laws to deal with that threat. Would you agree with that?

Mr. HOLDER. I think there are some changes we might want to consider with regard to existing law. There are problems, for instance, with the current jurisdictional limit, where Federal jurisdiction, criminal jurisdiction begins there is a $5,000 limit we have to meet. We think that is an artificially high limit.

The question of how we are able to use our technology to detect who is actually perpetrating these crimes, we have to, for instance, go from court to court to court as we are trying to trace back who engages in these kinds of attacks, and every time we go to a different State or a different jurisdiction we have to come up with a new court order, and the thought about maybe having a national court order that would allow us to get access to that information, I mean, there are a number of things that we are thinking about.

In terms of legislation we might propose, any legislation we propose would have to be balanced between the investigative needs that we have and the privacy interests that are really paramount in this area.

Senator WYDEN. I can tell you, I think the American people are going to be real concerned about the discussion about national court orders, legislation in that area. As you know, there is enormous concern right now about privacy, and it has now emerged as one of the two or three most important concerns to people.

And the reason I asked you the question about whether you think this is more of an enforcement issue rather than a question of needing new laws is that the whole history of these kinds of debates is that we have these threats, and particularly now, where we are clearly dealing with people who are not technologically simpletons—these are very, very sophisticated people—is that we have these attacks, and the call goes out for a variety of new laws, and very often I think there is the potential to have the cure worse than the ailment.

I guess I would ask next, what would you say to those who are troubled by the prospects that there could be further encroachments on privacy as a result of some of these ideas that you are advancing, and I was not familiar in detail with this national court order, and I follow this area pretty closely. What would you say to those who are concerned about the prospect that this could further erode privacy rights, and what assurance would you want to provide to them this morning?

Mr. HOLDER. Well, I would say first off the requests that we are considering are really ones that are, I think, very modest in scope. The notion, for instance, about the court order that would have Nation-wide effect, as we try to track these things down—somebody in New Jersey does something that attacks a network, a computer Web site in Oregon and runs it through Wisconsin and Texas.

As we go to try to trace this thing back, and time is important in trying to find out who is the perpetrator of this, we get to Wisconsin, we get to Texas, and each time we want to go back we have to get yet another court order.

Our proposal, one we are thinking about, is that we would have the ability to go to a judge and ask for an order that would allow us, as we get to these different States, not to have to go to get another judge to get essentially what the first judge has already given us.

I do not think that really encroaches on privacy, and I think that to assure people, I think everyone should understand that the proposals we are making are, as I said, very modest in scope, and are made by people who are very sensitive to the concerns that people have raised about privacy. The reality is, the Internet really can only be successful if those privacy interests are considered and, in fact, if they are protected.

Senator WYDEN. But understand as well that you are asking for powers that the Federal Government would have that largely expand the privacy threats to people already who are concerned about it in the private sector. Now, your obligation is obviously different than the obligations in the private sector, and I recognize that, but at the same time I think you are going to have to be very vigilant in terms of addressing these privacy issues.

And let me suggest a model that I talked about when we had the encryption debate, and one of the things that concerns me is that I do not want to see this discussion go the same route as that debate, where essentially we were gridlocked for years in terms of how to address both national security and the desire for companies to be able to export these products.

If the focus is primarily on enforcement, rather than the passage of new laws, I think having ongoing discussion with people in the private sector so that they can try to tell you how to get out in front of the innovation curve, so to speak, where the criminals are always more inventive and always more innovative, is the best way to deal with this, rather than to go out and try to advance new laws, which any way I look at it seem to give the Federal Government more power in areas that will raise privacy questions.

Mr. HOLDER. Well, I agree with you, we have to have that interaction with private industry and, as I have indicated, I think in terms of protecting the Internet, at least with regard to the initial parts of it, I think the responsibility should lie with private industry, but in terms of legislation, we have also thought about the proposal that what we would like to do is have electronic communications subject to the same consideration, the same kinds of privacy safeguards as oral and wire communications, so we would actually enhance the privacy considerations.

Senator WYDEN. I think those kinds of things will be well-received. Senator Burns and I have a privacy bill, and if that is the

kind of thing you are interested in, I think we would be very open to looking at something like that.

Even in the context of the privacy discussion it may not be solely within the province of our committee, but we are very hopeful. We have spent well over a year trying to develop a bipartisan privacy bill. We are very hopeful that we are going to be able to see progress on this and get it out on the floor of the Senate, given the public concern, and that is the kind of idea that I think makes a lot of sense, because in effect you do advance privacy rights.

You are addressing what is a concern of law enforcement, but I can tell you that if you stand up at a town hall meeting in my home State and start talking about national court orders and some of the other things that I have seen discussed, I think we may well end up with the same sort of gridlock we had on the encryption issue, and I do not want to see us go that route. There is too much goodwill, I think, in both the law enforcement community and in the private sector for us to just go back to that sort of encryption model, where everybody is gridlocked for years and years.

I felt for a long time that we were pursuing in the encryption area an approach that instead of a win-win was a lose-lose. It was not getting you what you needed in terms of law enforcement, and we were losing out in terms of international markets because we had this outdated standard in terms of the bit measure and the like for exports.

So let's pursue a different model. You give us ideas about the oral and written communication that make it easier for you to do your job and for us to be able to say in Montana and Oregon we are advancing people's privacy, and I think we are on our way to a winner, but some of these other suggestions I would urge you to be pretty cautious about.

Mr. HOLDER. I really think there is an ability, if we really talk with one another—there are I think sometimes instinctive reactions, negative reactions to the notion that we want to have additional legislation, and yet when we have interacted with industry and specifically told them these are the kinds of things we are thinking about, the reaction we have had has actually been pretty favorable, and people seem somewhat surprised when we say we also want to do things on the privacy side and have requirements that apply to wire and oral communications also apply to electronic communications.

I think that shows the necessary sensitivity that I think we have in the Government as we formulate these proposals.

Senator WYDEN. Clearly, a prospect that we can start bringing to the online world some of these approaches that we have used offline is a very, very promising orientation, and I like that.

What I think is going to raise the decibel level and generate much more controversy are some of these issues relating to court orders, the evidentiary standards that have been talked about concering how to gather some of this information, and the techniques for gathering it.

That is what I want us to be cautious about, because in that area I think we might harm privacy rights and, set back the legitimate businesses that you are understandably concerned about, as I am. The unintended consequences prospect is very much alive when

you talk about things involving evidence, techniques for gathering information, the court orders and the like. I appreciate your sensitivity and look forward to talking with you.

Thank you, Mr. Chairman.

Senator BURNS. Thank you.

You know, going along this same line, this may be the wrong question to the wrong panel, but instead of asking for new laws and new ways of pursuit of people who would hack, I go back to—we were raised—I bet every one of us sitting in here today, we were raised in a culture that even though we had open mail boxes out on the farm, you just did not touch another man's mail box because there was a Government warning there that you are violating the mails.

Do we have any way of posting warnings—FBI warnings on dubbing old VCR's, you know. Do we have any way of putting up there, it is a violation, a Federal violation to wander even into cyberspace in areas where you are unauthorized? I do not know, I am just thinking about it as he was talking about it. You know, the direction we are going, how do we know these people think that they are in violation of doing something and there are severe penalties for doing so?

Mr. HOLDER. I suppose there are technical ways to do that. I would really defer to industry as to how effective they think those kinds of things might be and whether, frankly, there might be some chilling effect in having those kinds of warnings, but again, it is not something I have really thought about.

Mr. VATIS. We do have banners on Federal computers that warn people who are coming into a system that if they are intruding without authorization, that constitutes a Federal crime, and that their activities that are subject to being monitored and investigated.

There are not, as far as I know, similar banners on all private sector systems, but it would certainly be technically feasible and fully legal for someone to put such a banner on a private sector system and say, "If you intrude into my system I will report the incident to law enforcement and I will seek to have you prosecuted if you violate Federal law."

Senator BURNS. Well, I am just saying, you know, even though we walked by our neighbor's mail boxes every day, you just did not fiddle around with another man's mail, and there was a post—every mail box we ever bought there was a Government message there, even though it was never locked or anything like that, and we were raised in that culture. You were taught that when you were a little child in your neighborhoods.

Mr. HOLDER. I think that is an important point, and a very good one, in that we need to do something with our young people in particular, but I think people more generally—people tend not to take the kinds of lessons that we learn with other things and apply them to the Internet.

There are privacy concerns that people have. There are certain things that you would not do in the material, the real world that people seem to do when it gets to the cyber world, or to the Internet, and we need to train people to make them more sensitive, make them aware that the kinds of don'ts, things you would not

do in the real world you should also not do when it comes to the cyber world, so it is a question, I think, of educating people and training them.

Senator BURNS. I was just thinking, in the conversation, the culture you were raised in, and that if you did monkey with somebody else's mailbox, they would usually beat you home and they called your mom and dad up and you got quite a beating when you got home.

But I just wonder if there is some way, even when signing on, if the operating bed or the operating system that you have got, there is not a warning that you have a certain responsibility, you are licensed to use this, but you have a certain responsibility that goes along with it. And I am wondering if something like that can be done and would scare off maybe some of the folks who would tend to wander into areas where they are not supposed to be.

We want to thank you for your testimony this morning. The industry comes up next. I want to beg of you to let us know, Members of Congress. It does not hurt, even in the security area, where we cannot discuss things maybe in an open forum, but we can in a private forum, either in your office or, it does not make any difference. But keep us abreast, if you would, of what is going on out here.

I am going to ask a question. How serious is this business? Extortion is a terrible, terrible thing that happens in any society. Is it a big problem in the Internet world?

Mr. VATIS. There have been numerous instances of extortion plots carried out via e-mail, and threats delivered by e-mail. There have also been specifically computer-related extortion efforts, where criminals have said, "Unless you pay me a certain amount of money, I am going to shut down your system or I am going to do something else to harm you."

Before these denial of service attacks took place, the last highly publicized example of a cybercrime was exactly that sort of extortion attempt, where somebody broke into a company called CD Universe (which sells CD's online), stole numerous credit card numbers from that company, and then threatened the company by saying that, unless CD Universe paid a certain amount of money, the hacker would post those credit card numbers on a Web site—which he subsequently did. That is another case that we have under investigation, but it is only one example of a rising trend in that sort of extortion scheme.

Senator BURNS. Well, that does not scare me much, because my wife keeps our credit cards right up to the limit, so they are not going to be OKed anyway. [Laughter.]

No, not really. She is coming back to town. We have got to clear that from the record. [Laughter.]

But I just wondered how bad that situation was, because I know that is a terrible, terrible, terrible crime. And thank you again this morning for your time and your testimony. We appreciate that very much. And if other Senators do have questions, I will direct them to you. And if you could respond to them and the committee, it would certainly help. And your full statements will be made part of the record. And we thank you for coming this morning.

We move now to the second panel, made up of Mr. Michael Fuhrman, who is Manager, Security Consulting, Cisco Systems, out of San Jose, California; Paul Misener, who is Vice President of Amazon, out of Seattle; and Raj Reddy, from Herbert A. Simon Professor of Computer Science and Robotics, Carnegie Mellon University, out of Pittsburgh, Pennsylvania.

Gentlemen, we appreciate you coming this morning and sharing your information with us. Again, you can summarize your statements, and rest assured that your full statements will be made a part of the record. Again, I thank you for coming this morning.

Mr. Misener, we will start off with you this morning.

STATEMENT OF PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM

Mr. MISENER. Good morning, Chairman Burns. It is very good to see you again, in particular. I thank you very much for inviting me.

My name is Paul Misener, and I am Amazon.com's Vice President for Global Public Policy. Amazon.com opened its virtual doors in July 1995, with a mission to use the Internet to transform book buying into the fastest, easiest, and most enjoyable shopping experience possible. Today, Amazon.com also offers consumer electronics, toys, CD's, videos, DVD's, home improvement tools, and much more. Seventeen million people in more than 160 countries have made us the leading online shopping site. And we also have a thriving auctionsite, Mr. Chairman.

Amazon.com greatly appreciates the opportunity to testify before your Subcommittee.

Senator BURNS. You are starving us old auctioneers to death.

[Laughter.]

Mr. MISENER. Please join us there.

Amazon.com greatly appreciates this opportunity to testify before your Subcommittee on the recent distributed denial of service attacks. We look forward to working with Congress to address these incidents and other important Internet policy issues.

Because the Internet and electronic commerce is the driving factor in the current booming economy, our Nation's economic well-being depends in part on stopping illegal activity that impedes e-commerce. We particularly support the Federal Government's involvement in fighting criminal behavior on the Internet. And we recognize and appreciate, however, your Subcommittee's important role in overseeing communications commerce.

Mr. Chairman, although the distributed denial of service incidents that occurred last month have been described many times in the press and elsewhere, a short description of what specifically happened to Amazon.com bears repeating. In essence, for about an hour on February 8, 2000, a large amount of so-called junk traffic was directed to our Internet site. This junk traffic degraded the technical quality of service at the site. To be clear, this was not a break-in at our online premises, but rather a deliberate and illegitimate crowding of virtual driveways and sidewalks around our online store. This crowding somewhat hinders our customers' ability to visit and shop.

At all times during this crowding, however, our customers' information was safe and secure, and many customers were able to

enter our store and shop. Nonetheless, for about an hour, our customers experienced congestion-related delays when visiting the site. For Amazon.com customers', who have come to expect the world's best online shopping experience, even such a relatively minor inconvenience was frustrating.

This is a key point for these hearings, Mr. Chairman. Consumers are the ones inconvenienced by distributed denial of service attacks. Indeed, millions of consumers have come to rely on the Internet to communicate, shop, invest, obtain news, and learn online. The denial of service attacks last month interrupted these important consumer activities and, thus, it is on behalf of consumers that all of us must work to prevent these attacks in the future.

So what can the Federal Government do about denial of service attacks? Amazon.com believes the Government's key role should be to prosecute the perpetrators of these and other online criminal activities. Currently laws have been used successfully in recent cases. In addition, some have suggested extending existing laws or enacting new laws, and others have suggested establishing stiffer penalties under existing statutes.

On behalf of our current and future customers, Amazon.com would be happy to work with Congress on any new legislation to address Internet crime issues.

Successful prosecutions, of course, also rely on adequate resources with which to conduct investigations. Amazon.com believes that additional resources should be applied in at least four areas: law enforcement training, personnel retention, public education, and agency coordination.

Let me say a few things about each area. First, continuous training of law enforcement personnel in the latest digital forensic techniques, as well as current Internet technologies, should be at the top of any list for additional funding. In particular, additional training in electronic evidence handling is necessary, for preservation of digital evidence is as important for cybercrime prosecutions as preservation of fingerprints is for physical crimes.

Second, given the strong demand for information technology experts, both within and outside of Government, law enforcement agencies need additional resources to retain senior IT professionals and attract new ones.

Third, Federal law enforcement agencies should have sufficient resources to help educate private industry and consumers on preventing Internet-related crime.

Finally, better coordination and communication among Federal, State, local, and international law enforcement agencies is needed. The recent incidents were not geographically localized, and there is no reason to expect future Internet crime to be.

In all of these areas, increased Government interaction with private industry would help. Amazon.com already is engaged in this sort of informal partnership. In addition to existing ongoing investigations, our technologists are working with various law enforcement personnel on the latest developments in Internet technology and techniques. We believe it would be premature, however, to formalize this partnership.

Absent from our suggested Federal response is a role for the Federal Communications Commission. The reason is straightforward:

The distributed denial of service attacks involved coordinated and criminal transmission of content over the Internet. It is hard to see how the FCC has statutory authority over such matters. And even if it had or were given such authority, the agency currently lacks the resources and expertise to do what is necessary at this point; namely, to fight the criminal activity.

Simply put, useful FCC involvement would require statutory changes, additional resources and additional expertise to succeed. This is work better left to law enforcement agencies.

In conclusion, Mr. Chairman, we applaud your effort to address these denial of service attacks and to formulate an appropriate Federal response. As indicated, we believe the situation currently is best handled using law enforcement mechanisms. But we would appreciate your Subcommittee's continued interest in the matter.

On behalf of our current and future customers, Amazon.com stands ready to help. Thank you very much for the opportunity to testify before your Subcommittee. I would be pleased to answer your questions and I look forward to working with you.

[The prepared statement of Mr. Misener follows:]

PREPARED STATEMENT OF PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM

My name is Paul Misener, and I am Amazon.com's Vice President for Global Public Policy. Amazon.com opened its virtual doors in July 1995 with a mission to use the Internet to transform book buying into the fastest, easiest, and most enjoyable shopping experience possible. Today, Amazon.com also offers consumer electronics, toys, CDs, videos, DVDs, home improvement tools, and much more. Seventeen million people in more than 160 countries have made us the leading online shopping site.

Amazon.com greatly appreciates the opportunity to testify before your Subcommittee on the recent distributed denial of service attacks. We look forward to working with Congress to address these incidents and other important Internet policy issues. Because electronic commerce is the driving factor in the current booming economy, our nation's economic well-being depends in part on stopping illegal activity that impedes e-commerce.

We particularly support the Federal Government's involvement in fighting criminal behavior on the Internet. We recognize and appreciate, however, your Subcommittee's important role in overseeing communications commerce.

Mr. Chairman, although the distributed denial of service incidents that occurred last month have been described many times in the press and elsewhere, a short description of what specifically happened to Amazon.com bears repeating.

In essence, for about an hour on February 8, 2000, a large amount of so-called "junk traffic" was directed to our Internet site. This junk traffic degraded the technical quality of service at the site.

To be clear: this was not a break-in at our online premises but, rather, a deliberate and illegitimate crowding of the virtual "driveways and sidewalks" around our online store. This crowding somewhat hindered our customers' ability to visit and shop.

At all times during this crowding, however, our customers' information was safe and secure, and many customers were able to enter and shop at our store. Nonetheless, for about an hour, our customers experienced congestion-related delays when visiting the site. For Amazon.com's customers, who have come to expect the world's best online shopping experience, even such a relatively minor inconvenience was frustrating.

This is a key point for these hearings: *consumers* are the ones inconvenienced by distributed denial of service attacks. Indeed, millions of consumers have come to rely on the Internet to communicate, shop, invest, obtain news, and learn online. The denial of service attacks last month interrupted these important consumer activities and, thus, it is on behalf of consumers that all of us must work to prevent these attacks in the future.

So what can the Federal Government do about denial of service attacks? Amazon.com believes the Government's key role should be to prosecute the perpetrators

of these and other online criminal activities. Current laws have been used successfully in recent cases. In addition, some have suggested extending existing law or enacting new laws, and others have suggested establishing stiffer penalties under existing statutes.

On behalf of our current and future customers, Amazon.com would be happy to work with Congress on any new legislation to address Internet crime issues.

Successful prosecutions, of course, also rely on adequate resources with which to conduct investigations. Amazon.com believes that additional resources should be applied in at least four areas: law enforcement training, personnel retention, public education, and agency coordination. Let me say a few things about each area.

First, continuous training of law enforcement personnel in the latest digital forensic techniques, as well as current Internet technologies, should be at the top of any list for additional funding. In particular, additional training in electronic evidence handling is necessary, for preservation of digital evidence is as important for cybercrime prosecutions as preservation of fingerprints is for physical crimes.

Second, given the strong demand for information technology experts, both within and outside of Government, law enforcement agencies need additional resources to retain senior IT professionals and attract new ones.

Third, Federal law enforcement agencies should have sufficient resources to help educate private industry and consumers on preventing Internet-related crime.

Finally, better coordination and communication among Federal, state, local, and international law enforcement agencies is needed. The recent incidents were not geographically localized, and there is no reason to expect future Internet crime to be.

In all of these areas, increased Government interaction with private industry would help. Amazon.com already is engaged in this sort of informal partnership: in addition to assisting the ongoing investigations, our technologists are working with various law enforcement personnel on the latest developments in Internet technology and techniques. We believe it would be premature, however, to formalize this partnership.

Absent from our suggested Federal response is a role for the Federal Communications Commission. The reason is straightforward: the distributed denials of service attacks involve coordinated and criminal transmission of content over the Internet. It is hard to see how the FCC has statutory authority over such matters. Yet even if it had, or were given, such authority, the agency currently lacks the resources and expertise to do what is necessary at this point, namely, to fight the criminal activity. Simply put, useful FCC involvement would require statutory changes, additional resources, and additional expertise to succeed. This is work better left to law enforcement agencies.

In conclusion, Mr. Chairman, we applaud your effort to address these denials of service attacks and to formulate an appropriate Federal response. As indicated, we believe the situation currently is best handled using law enforcement mechanisms, but we would appreciate your Subcommittee's continued interest in the matter. On behalf of our current and future customers, Amazon.com stands ready to help.

Thank you very much for the opportunity to testify before your Subcommittees. I would be pleased to answer your questions and I look forward to working with you.

Senator BURNS. Thank you very much, Mr. Misener.

Now we have Michael Fuhrman, who is Manager, Security Consulting, Cisco Systems. Welcome before the Subcommittee. We look forward to your testimony.

STATEMENT OF MICHAEL FUHRMAN, MANAGER, SECURITY CONSULTING, CISCO SYSTEMS

Mr. FUHRMAN. Thank you, Chairman Burns.

I am Michael Fuhrman of Cisco Systems. As you know, Chairman, we are the largest manufacturer of equipment that connects people and businesses to the Internet. We are based in San Jose, California, and we have large operations in Massachusetts, North Carolina and Texas.

Senator BURNS. Did you ever consider Montana?

[Laughter.]

Mr. FUHRMAN. We do have sales offices in Montana, yes.

In particular, I manage our company's Security Consulting Services Group, which helps to ensure the security of some of the best known sites on the Internet. My team of engineers and specialists evaluate the protective measures being employed by our customers. We help them respond to anyone or anything that threatens the integrity of their systems. And as last month's hacker attacks on some of the world's busiest Web sites graphically demonstrated, this is a task that requires constant vigilance.

Cisco security specialists were among those who responded to the denial of service attacks that temporarily blocked access to several sites, beginning on February 7th. I am happy to tell you that we were able to help some of our customers quickly identify the technology being used in the attacks, employ effective countermeasures, and beat back repeat efforts by hackers to obstruct access.

Now, in a nutshell, the hackers initially were able to briefly shut customers out of some targeted Web sites, as Mr. Misener said, by bombarding these sites with more information than they could process at the time. In a way, we liken it to the Internet equivalent of trying to go shopping the day after Thanksgiving. The crowds are overwhelming and the parking lots are full. The difference in this case is, however, that people were not prepared for this activity.

Now, after these assaults, there was some heated speculation about whether the public can depend on the Internet as a reliable means of doing business and sharing information. Now, the lesson to be learned from the attacks is not that the hackers have some sort of technological edge. On the contrary, the technology that is employed in these attacks is well-known to those of us in the systems security field. Proper defenses for a majority of these, the technology does exist.

The lesson is that events like this can be anticipated and managed with the proper diligence and planning. The technology community showed that it can respond swiftly and effectively, taking steps to quickly mitigate the attacks and to make it harder for future attacks in the future.

Now, it is important to note, in all of these assaults, targeted Web sites were interrupted only for relatively brief periods. It is also important to note, again, as Mr. Misener stated, these attacks blocked access to some systems, but did not penetrate into the internal systems of these companies.

The technology community has already joined with the Federal Government to respond more effectively should attacks like these be repeated in the future. The community and the Government are forming an organization that will disseminate critical information quickly and widely if the Internet is threatened.

We at Cisco keenly understand the importance of this task. We will conduct $12 billion of business over our Web site this year. Our employees perform 95 percent of their tasks on our Web site. My consulting group in particular recently conducted a 6-month survey of 33 businesses connected to the Internet, where we measured their state of security. We found that, on average, one out of every three of the companies' devices connected to the Internet were vulnerable to some form of attack or another.

We also found, however, that 90 percent of the vulnerabilities could be solved with technology that was readily available today, if the technology is properly employed and consistently updated. Now, this, of course, is easy to say and extraordinarily difficult to do.

We have to remember that a decade ago the Internet was little more than a clunky mechanism that a few educational research institutions used to trade messages we now all know as E-mail. The blazing speed at which the Internet has developed and the equally rapid pace at which threats to the Internet's security have evolved make it hard even for those who build and maintain Web sites to keep pace.

But businesses and others who operate Web sites are learning that security must become an ever more important concern. The number of companies who come to Cisco, for instance, in assistance in securing their networks has grown by over 50 percent over the last 12 months alone—a very encouraging statistic. And we have all learned that one thing the technology can do collectively is to increase the sharing of information about up-to-the-minute developments in security.

We believe that this public/private partnership is the most effective response to the recent attacks. In the private sector, incentives must be put into place to encourage all Web sites to deploy security technologies, to protect themselves and their customers from hacker attacks. In the public sector, we are grateful that the Federal Bureau of Investigation has devoted significant resources to investigating these attacks. And we hope that the perpetrators will be prosecuted to the fullest extent of the law.

We encourage the Federal Government to serve as a role model for private industry, by equipping its own computer systems with the best security measures possible. This, too, of course, will not be easy. Both the Government and private enterprise are having difficulty attracting and retaining enough skilled professionals in the field of systems security. I am happy to tell you that the private sector has joined with the Office of Personnel Management to help the Government in the area by developing training and mentoring programs. Again, we regard this as an excellent example of public/private partnership.

At this time, however, we do not ask Congress for new laws in the area of Internet security. Cooperation, not regulation, not legislation, will ensure that the Internet remains secure and, at the same time, open to the broadest public access. The Internet is and always should remain an open medium. No one can insulate the Internet and everything connected to it from all threats, or guarantee that no attack on any particular Internet site will succeed.

Even our oldest, most established public infrastructures pause on occasion. Power and telephone lines come down, water mains break, highways become clogged. And like them, the Internet will occasionally have localized difficulties. These are but potholes on the information superhighway, which we will fill in as fast as they appear, learning how to prevent similar potholes in the future.

The recent attacks actually demonstrated that the technology community can quickly identify threats to the Internet, quickly act to eliminate them, and quickly take measures that will reduce the

impact of similar threats in the future. This spirit of innovation and rapid development propels the Internet's exponential growth and ensures that the Internet will remain secure as it continues to grow.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Fuhrman follows:]

PREPARED STATEMENT OF MICHAEL FUHRMAN, MANAGER, SECURITY CONSULTING, CISCO SYSTEMS

Chairman Burns and distinguished senators, I am Mike Fuhrman of Cisco Systems. As you may know, Cisco is the world's largest manufacturer of equipment that connects people and businesses to the Internet. We are based in San Jose, California and have substantial operations in Massachusetts, North Carolina and Texas.

I manage our company's Secure Consulting Services Group, which helps ensure the security of some of the best-known sites on the Internet. My team of engineers and specialists evaluates the protective measures being employed by our customers and helps them respond to anyone or anything that threatens the integrity of their systems. As last month's hacker attacks on some of the world's busiest web sites graphically demonstrated, this is a task that requires constant vigilance.

Cisco's security specialists were among those who responded to the so-called "denial of service attacks" that temporarily blocked access to several web sites beginning Feb. 7. I'm happy to tell you that we were able to help some of our customers quickly identify the technology being used in these attacks, employ effective countermeasures and beat back repeat efforts by hackers to obstruct access.

In a nutshell, hackers initially were able to briefly shut customers out of some targeted web sites by bombarding those sites with more information, some of it more false or misleading, than they were able to process. In a way, it was the Internet equivalent of trying to shop on the day after Thanksgiving, when the crowds are overwhelming. But in this case, the problem was nobody knew the rush was coming and therefore we weren't quite prepared to handle it.

After these assaults, there was some overheated speculation about whether the public can depend on the Internet as a reliable means of doing business and sharing information. The lesson to be learned from these attacks is *not* that hackers have some kind of technological edge that enabled them to do what they did. On the contrary, the technology employed in these attacks is well known to those of us in the systems security field and proper defenses against that technology are widely available.

The lesson is that events like these can be anticipated and managed with diligence and proper planning. The technology community showed that it can respond swiftly and effectively, taking steps to quickly mitigate the attacks and to make it harder for similar assaults to succeed in the future.

It's important to note that, in all of these assaults, service to targeted web sites was interrupted only for relatively brief periods. It's also important to note that while these attacks blocked access to some targeted computer systems, they do not appear to have penetrated the outer defenses of these systems. We know of no case in which hackers obtained access to confidential customer information, such as credit card numbers, or did lasting damage to any of the targeted sites.

And it's important to note that the technology community has already joined with the Federal Government to respond more effectively should attacks like these be repeated in the future. The community and the Government are forming an organization that will disseminate critical information quickly and widely if the Internet is threatened.

We at Cisco Systems keenly understand the importance of this task. We will conduct $12 billion worth of business over our own web site this year, and our employees are able to perform about 95 percent of their work on the site.

Cisco Secure Consulting Services recently conducted a six-month survey of 33 businesses connected to the Internet and measured their "state of security." We found that, on average, one out of every three devices connected to the Internet was vulnerable to some form of attack. But we also found that over 90 percent of the vulnerabilities could be solved with technology that is readily available, if the technology is properly employed and constantly updated.

This is easy to say and extraordinarily difficult to do. A decade ago, the Internet was little more than a clunky mechanism that a few educational and research institutions used to trade messages we now know as email. The blazing speed at which the Internet has developed—and the equally rapid pace at which threats to Internet

security have evolved—make it hard even for those who build and operate web sites to keep pace.

But businesses and others who operate web sites are learning that security must become an ever-more-important concern. The number of companies who have come to Cisco for assistance in securing their networks has grown by over 50 percent during the last 12 months alone—a very encouraging statistic. And we have all learned that one thing the technology community can do collectively to increase is to share information about up-to-the-minute developments in systems security.

The community has joined with the Federal Government to do just this. Even before last month's attacks, industry leaders had joined to form the Partnership for Critical Infrastructure Security. The PCIS is a voluntary organization that is working to share information about threats to the Internet and other crucial networks, and determine how best to respond to those threats. About 120 companies are cooperating in this effort.

And last month at the White House information technology summit, Cisco was one of about 40 Internet companies that agreed to develop a structured mechanism to react to events like the recent hacker attacks. As with the PCIS, industry is coordinating its activities with the Federal Government.

We believe that this public-private partnership is the most effective response to these recent attacks. In the private sector, incentives must be put into place to encourage all web sites to deploy security technologies to protect themselves and their customers from hacker attacks.

In the public sector, we are grateful that the Federal Bureau of Investigation has devoted significant resources to investigating these attacks and we hope the perpetrators will be prosecuted to the fullest extent of the law. We encourage the Federal Government to serve as a model for private industry by equipping its own computer systems with the best security measures possible.

This, too, will not be easy. Both the Government and private enterprise are having difficulty attracting and retaining enough skilled professionals in the field of systems security. I'm happy to tell you that the private sector has joined with the Office of Personnel Management to help the Government in this area by developing training and mentoring programs. Again, we regard this as an excellent example of public-private partnership.

At this time, however, we do not ask Congress for new laws in the area of Internet security. Cooperation, not regulation or legislation, will insure that the Internet remains secure and at the same time open to the broadest possible public access.

The Internet is, and should always remain, an open medium. No one can insulate the Internet and everything connected to it from all threats or guarantees that no attack on any particular Internet site will succeed. Even our oldest, most established public infrastructures pause on occasion—power and telephone lines come down, water mains break, highways become clogged—and, like them, the Internet will occasionally have localized difficulties. These are but potholes on the information superhighway, which we will fill in as fast as they appear—learning how to prevent similar potholes in the future.

These recent attacks actually demonstrated that the technology community can quickly identify threats to the Internet, quickly act to eliminate them and quickly take measures that will reduce the impact of similar threats in the future. This spirit of innovation and rapid development propels the Internet's exponential growth and ensures that the Internet will remain secure as it continues to grow.

Thank you. I look forward to your questions.

Senator BURNS. Thank you, Mr. Fuhrman.

Dr. Reddy, welcome to our Subcommittee.

And can I get your statement right after this?

Senator ABRAHAM. Why do we not let him go.

Senator BURNS. I think that is wise. Thank you.

Dr. Reddy, thank you very much for coming this morning. We look forward to your testimony.

STATEMENT OF RAJ REDDY, PH.D., HERBERT A. SIMON PROFESSOR OF COMPUTER SCIENCE AND ROBOTICS, CARNEGIE MELLON UNIVERSITY

Dr. REDDY. Thank you, Mr. Chairman. This is a great opportunity for us to testify before the Subcommittee.

My name is Raj Reddy. I am the Herbert A. Simon Professor of Computer Science and Robotics at Carnegie Mellon University. I also serve as the Co-Chair of the President's Information and Technology Advisory Committee, commonly known as PITAC.

In the PITAC February 1999 report to the President, labeled "Information Technology: Investing in our Future," we highlighted the need for increased investments in national security—about 15 months ago—as well as a number of other research areas.

Today, on behalf of PITAC, I will provide you with insights into the state of the Internet security in our country and outline some of the PITAC recommendations that will help our Nation to build and support a more reliable, available, secure, and scalable Internet. I will also provide some personal observations on, besides legal and administrative remedies, what research and technology remedies might exist to solve this problem of denial of service.

While advances in information technology have created unprecedented economic growth and transformed our lives in thousands of positive ways, weaknesses still remain that enable malicious hackers to disrupt Internet service and overload popular Web sites. An analysis of these highly visible disruptions to the Internet reveals a wide range of causes, including denial of service from hackers.

The PITAC shares Congress' concern about these recent hacker attacks. In our February 1999 report, we observed that the Internet has grown well beyond the intent of its original designers 25 years ago, and that our ability to extend its use has created enormous challenges. In our report, we recommended a research agenda to help ensure the survivability of our information infrastructure in the face of malicious attacks, equipment and software failures, and legal overload, where a large number of people call in a Schwab account site on a busy stock market day.

We concluded that the support for critical, long-term fundamental research in IT is diminishing, and that the current research is too focused on near-term problems related to agency missions. To help maintain the U.S. leadership in IT, information technology, and restore a commitment to high-risk, high-return research, we recommended that the Federal Government create a strategic initiative in long-term R&D funding, and increase the funding for R&D over the next 5 years by $1.4 billion.

Our report recommended a balanced research agenda in software, scalable information infrastructure, high-end computing, and work force implications. Specifically, we recommended research to support scalable information infrastructure, authentication and security mechanisms, mechanisms for detecting system intrusion, mechanisms for detecting mitigating and responding and recovering from human error in the creation and the use of the infrastructure, mechanisms for assuring information quality, and a number of others.

PITAC is encouraged by the strong bipartisan support for the information technology research and development and by the $235 million increased appropriation this year for the Federal IT R&D programs. Based largely on our recommendations, the administration proposal for the fiscal year 2001 budget includes a $600 million increase in investments for a balanced information technology

R&D program, which includes funding for networking and software research to enable more secure, reliable, dependable networks.

We applaud the Senate's past leadership in supporting this information technology R&D, and we hope you will support the full set of research priorities we recommended in our report.

Now I would like to make some personal observations on the specific problem of Internet security. Remedies to the problems of denial of service attacks and security loopholes and insider risks, there are a number of different ways of skinning this cat. One is legal; the other is administrative; and, finally, there is also an opportunity to use research and technology to stop many of these problems. And I would like to share with you some ideas on that topic.

I propose that we establish a national network test bed that can be used to develop and demonstrate what I will refer to as an ultra-dependable, self-healing Internet. The purpose of this test bed is to try out new approaches without disrupting the crucial production infrastructure. It is an R&D vehicle. The proposed test bed will be similar to the ultra high-speed network test bed, NGI, Next Generation Internet, that has been funded in the last few years.

It will include attributes such as reliability, availability, scalability, in addition to security. The operative issue is not security alone, as interpreted narrowly, but how to create a dependable Internet that we can all trust, like we trust the telephone system today. The ultra-dependable Internet would be used to develop technologies to enable self-healing networks.

A self-healing network would work similar to the human immune system. It would continuously monitor the system—in this case, the network—analyze what is happening in the system, what packets are going through, and it would detect abnormal patterns automatically and immediately begin actions to remedy this problem. It would use software agents, capable of self-monitoring, self-diagnosing, and self-repair, much as the human immune system uses distributed antibodies to disable antigens and restore balance in the human body.

Just as in the human system, where a few people may occasionally get sick but the society as a whole continues to function, we may accept an occasional denial of Internet service in a particular location, as long as most of the users are able to access most of the Web sites most of the time without any degradation of service. The proposed self-healing network will increase the packet handling overhead and perhaps make the system slower. We believe, with the exponential growth in technology, this will not be a serious problem in the future.

In addition to the research needed to develop the faster networks, we will also need research in data warehousing of metadata contained in the packet headers, data mining of the statistical parameters that would classify normal and abnormal traffic, and repair strategies for generating signals that would make abnormal requests detectable.

In conclusion, I believe the creation of a dependable Internet infrastructure, as dependable as the telephone service, is essential to the future of the economic growth and security of this Nation. To accomplish this, we need bold new research initiatives and uniform

application of ideas across the international Internet infrastructure. Support for the increased Federal investments in IT R&D is a positive first step. But continued dialog among Federal researchers, industry and academia is essential to create bold new ideas like a self-healing, dependable information infrastructure.

In summary, Mr. Chairman, it is estimated that the market capitalization of the Internet-based industries created since 1990 exceeds $1 trillion, resulting in capital gains taxed paid to the Nation of over $200 billion. Investing a small fraction of this national income in research toward creating an ultra-dependable, self-healing Internet will help ensure the continuation of this engine of growth.

Thank you.

[The prepared statement of Dr. Reddy follows:]

PREPARED STATEMENT OF RAJ REDDY, PH.D., HERBERT A. SIMON PROFESSOR OF COMPUTER SCIENCE AND ROBOTICS, CARNEGIE MELLON UNIVERSITY

Introduction

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to testify about important research and development efforts aimed at increasing Internet security and protecting our Nation's Information Infrastructure.

My name is Raj Reddy, and I am the Herbert A. Simon University Professor of Computer Science and Robotics at Carnegie Mellon University. I also serve as Co-Chair of the President's Information Technology Advisory Committee, commonly known as PITAC. In the PITAC's February 1999 report to the President, "Information Technology Research: Investing in Our Future," we highlighted the need for increased investment in network security, as well as other important research areas. Today, on behalf of PITAC, I will provide you with insight into the state of Internet security in our country and outline some of the PITAC recommendations that will help our Nation build and support a more reliable, available, secure, and scalable Internet. I will also present my personal views on an R&D strategy for developing and demonstrating highly dependable networks.

Background

While advances in information technology have created unprecedented economic growth and transformed our lives in thousands of positive ways, weaknesses still exist that enable malicious hackers to disrupt Internet service and overload popular Web sites. An analysis of the highly visible disruptions to Internet access reveals a wide range of causes, including denial of service attacks from malicious hackers using insecure hosts infected with "zombie" diseases (Yahoo!), software bugs (Ameritrade), insecure configurations (Schwab), change management (E-trade), and security loopholes (Hotmail, Melissa).

PITAC shares Congress' concern about these recent hacker attacks. In our report to the President, we observed that "the Internet is growing well beyond the intent of its original designers and our ability to extend its use has created enormous challenges. As the size, capability, and complexity of the Internet grows, it is imperative that we do the necessary research to learn how to build and use large, complex, highly-reliable, and secure systems . . . It is therefore important that the Federal Government undertake research on topics ranging from network reliability and bandwidth, to robust, reliable, secure ways to deliver and to protect critical information." In our report, we recommended a research agenda to help ensure the survivability of our information infrastructure in the face of malicious attacks or viruses, equipment or software failures, and overload. Before I discuss the specifics of the R&D agenda for Internet security, I would first like to briefly summarize the findings and recommendations of our report.

The PITAC Report Findings and Recommendations

The PITAC was established pursuant to the High Performance Computing Act of 1991 and was tasked to look at a number of issues in high performance computing and communications. After a detailed review of the Federal IT R&D programs, we concluded that U.S. leadership in IT provides an essential foundation for promoting economic growth, education and research, environmental stewardship, public health, and national security. We also concluded that there has been an erosion of support for long-term fundamental research in IT and that current research is too focused

on near-term problems linked to agency missions. Our Committee recommended that the Federal Government create a strategic initiative for long-term R&D and increase funding for IT R&D by $1.4 billion by fiscal year 2004 over the fiscal year 1999 base programs funding level. Our report recommended a balanced research agenda, with priority for the following areas:

- Software: Methods for efficiently creating and maintaining high-quality software of all kinds and for ensuring the reliability of the complex software systems that now provide the infrastructure for much of our Government and our economy.
- Scalable Information Infrastructure: Techniques for ensuring that the National Information Infrastructure consisting of communications systems, the Internet, large data repositories, and other emerging systems is reliable and secure, and can grow gracefully to accommodate the massive numbers of new users (perhaps billions) and applications expected over the coming two decades.
- High End Computing : Continued invention and innovation in the development of fast, powerful computing systems and the accompanying communication systems are needed to implement critical science, engineering, and business applications ranging from aircraft design to weather and climate modeling.
- Social, Economic, and Workforce Implications of IT: Research directed towards better understanding the sociological and economic impacts of innovations in information technology and toward growing the workforce to meet the national need for information technology professionals.

Our recommendation for research to support a scalable information infrastructure included topics to enable the survivability of our networks and information. Survivability means that services will be available when needed and information will be delivered in a timely fashion. The recommended research agenda includes:

- Authentication and security mechanisms for a large, heterogeneous, and evolving infrastructure
- Mechanisms for detecting system intrusion and information software corruption
- Mechanisms for detecting, mitigating, responding to, and recovering from, or for preventing, human error in the creation and use of the infrastructure
- Mechanisms for assuring information quality
- Scalable information and service replication strategies
- Mechanisms for monitoring services to ensure correct operation within given quality-of-service bounds
- Repositories for guaranteed long-term preservation of information

Our report recommendations have received strong bi-partisan support and we were encouraged by the $235 million increase for IT R&D appropriated in this year's budget. The President's fiscal year 2001 budget proposes an increase of nearly $600 million in IT R&D in a balanced research program that addresses the recommendations in the PITAC report. Proposed funding includes networking and software research directed towards technologies to enable more secure, reliable, and dependable networks. The PITAC applauds the Senate's past support and leadership for IT R&D and hopes the Senate will support the full set of research priority areas recommended in our report.

The PITAC report provides broad concepts for a balanced IT R&D program. While we recognized the importance of network security, reliability, and dependability, we did not develop a detailed R&D agenda for Internet security. Our recommendations cover a range of important topics to be addressed, rather than proposals for specific research projects.

The Impact of Internet Downtime on Businesses and Society

Denial of service happens when the network fabric is overloaded through intentional and unintentional ("legal") overloading of the system with too many requests. This is analogous to a large number of people calling California in the event of an earthquake report, or a computer calling a phone continuously thereby blocking anyone else getting through in case of an emergency. The cost of denial of service and overloading can be substantial. The Yankee Group estimates that the online industry may have lost $1.2 billion in revenue from the Web site attacks earlier this month. (*WSJ,* Feb 24, 2000). A Gartner Group study showed that the average cost of downtime in brokerage operations is about $6.5 million per hour! According to the Boston-based market research firm, $29 million in refunds were paid out by MCI to customers affected by the 10 day outage of its frame relay network in August 1999. Three thousand companies were affected. (*Online News,* 10/28/99). eBay paid $3.9 million in credits to its customers for the service outage that halted bid-

ding completely at its popular service for an unprecedented 22 hours in June 1999. Distributed network sites can lose $20,000 to $80,000 per hour. (*Computer Reseller News,* 1998). At a cost of $80,000 per hour, the average company will lose $7.1 million per year in centralized network downtime.

These costs are expected to increase as companies incur indirect costs in the form of lawsuits, regulatory scrutiny, impact on brand name and public image, loss of customer base, lower employee morale and productivity, and higher employee stress.

The impact on businesses of system outage can be even more devastating. In an April 1999 survey of consumers, research firm Jupiter Communications found that 46 percent leave a preferred site if they experience technical or performance problems. Statistics from McGladrey and Pullen show that for every five organizations affected by a disaster, two will be unable to maintain their critical business functions and make a recovery. Of the remaining three, one will not survive the next two years. In fact, a company that experiences a computer outage lasting more than 10 days will never fully recover financially ("Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems" by Jon Toigo).

According to Cahners in-stat group, Internet downtime hits businesses financially, (http://www.instat.com/abstracts/ia/1999/is9906sp—abs.htm), affecting direct revenue/customer base, compensatory payments, inventory cost, and depreciation of capital. It also affects business in ways not seen on the balance sheet, such as market capitalization loss, employee downtime, and delays to market items that may prove more financially damaging than the explicit losses associated with an outage. The report "Data Failure: The Financial Impact on Internet Business" quantifies the real-cost damages for site outages based on SEC filings and publicly released information. The report compares two e-commerce business models and illustrates how much is at stake in the event of data failure.

Steps Towards a Secure and Dependable Internet

Many of the problems of Internet access can be avoided by taking some simple common sense precautions. For example:

Online businesses can:

- Educate users on cyber hygiene, security tools, and procedures such as use of the firewalls, intrusion detection systems, anti-virus software, automatic daily disinfecting tools, etc.
- Discourage masquerading and spoofing attacks by ensuring that network traffic exiting from the local area network of an organization carries the address consistent with the valid set of addresses for that organization.
- Protect against inside hacker risk by providing backup and retrieval from an off-site storage service provider. Disaster tolerance backup facilities are offered by many suppliers. Such services guarantee constant availability of data in the face of technical or natural catastrophe, including surge capabilities for unplanned swells in site traffic.
- Provide 24 hour-per-day, 7 day-a-week physical security to central facilities and server farms. Alternatively, use the backup and retrieval from an off-site storage service as described in the previous bullet.

Industry can:

- Release hardware and software that prevents insecure configurations, and provide tools for intrusion detection.
- Re-engineer operating systems and applications to make them immune to the effects of viruses and other forms of malicious code.
- Identify and close the security loopholes and backdoors by working with major vendors to provide access to the source code and encourage open source movement.
- Develop and deploy a secure communications infrastructure that can be used by network operators and Internet service providers to enable real-time collaboration when dealing with attacks.

Many of the common sense measures listed above depend on the voluntary compliance of more than a 100 million Internet users and organizations that provide Internet service. However, history has shown us that compliance failures will occur, either unintentionally or maliciously. Rather than leaving the Internet vulnerable because a few persons or organizations are careless or reckless, we should develop an information infrastructure that is not dependent on voluntary compliance of security practices and policies.

Personal Views on a Strategy for a National Self Healing Network Testbed

I would now like to make some personal observations and make a specific recommendation for creating a national self healing network testbed. The PITAC recommended an aggressive new program in networking research, including network security. We also recommended expanded research to explore ways that laws protecting privacy, intellectual property, and other rights are extended effectively into this new media. We continue to support increased funding in these critical areas.

The PITAC is currently reviewing Federal research plans and will be issuing new recommendations later this year. Since these new recommendations are not available, I would like to present my personal views on logical next steps.

By now we understand the sources of highly publicized Internet crashes: malicious hacker attacks and "legal" users overloading popular web sites. Many of the remedies require straightforward implementation of known solutions, either administrative or legal. However, herein lies the problem—we simply cannot depend on every system to be properly administered or every person to behave as desired. Instead, we should strive to develop an Internet infrastructure in which it does not matter if someone is careless or reckless. In my view, one of the key goals of networking research over the next few years should be development of a "self healing" network. A self healing network would work similar to the human immune system. It would constantly monitor the system (in this case, the network), analyze what is in the system, and if it finds something wrong within the system, immediately begin actions to remedy the problem. A self healing network would be capable of self-monitoring, self-diagnosing and self-repairing. To accomplish this, we should establish a national network testbed that can be used to develop and demonstrate what I will refer to as an "ultra-dependable Internet." This is similar to an ultra-high speed network, but with the focus on dependability rather than speed.

I will use the phrase "dependable Internet" to specifically include attributes such as reliability, availability, and scalability in addition to security. The operative issue is not "security" as interpreted narrowly in the research circles but rather "how to create a dependable Internet Infrastructure" that is as reliable as the current telephone system. By dependable, I mean a system ("as if my life depended on it") that is:

- **reliable,** i.e., always up, accessible, accurate, and consistent,
- **available,** i.e., a system with no world-wide-wait and a response time of under 200 milliseconds most of the time,
- **scalable,** i.e. an infrastructure capable of scaling to a billion simultaneous users and a trillion inter-connected devices, and
- **secure,** i.e. no fear of loss of privacy and immunity to sniffing and spoofing.

The goal of a self healing network is to provide mechanisms for detecting unauthorized use of networking equipment, tracking inappropriate uses, and identifying the individuals using networks for malicious intent, without compromising individual rights to privacy and security on the network. Over the years we have found ways to balance privacy and security in traditional commerce. Applying these precedents to the new networked world will require combining the skills of technologists and people knowledgeable of the legal, economic, and social issues. Clearly this is an enormous challenge, but I believe it is a critical national research challenge and deserves an appropriate response.

A Self Healing Network

A self healing network is one which continuously monitors all the traffic within the system (every packet entering the system is validated before it can proceed) with a view to detect and disable abnormal traffic patterns. It is predicated on using "software agents" capable of self-monitoring, self-diagnosis, and self-repair much as the human immune system uses (distributed) anti-bodies to disable antigens and restore balance in the human body. Just as in human systems where a few people may get sick some of the time, but society as a whole continues to function, we may accept an occasional denial of service as long as most users are able to access most of the web sites without any degradation of service.

Self monitoring within the Internet core fabric requires agents capable of continuous and autonomous monitoring of "packet" traffic using "software sensors." "Self repair agents" undertake a set of autonomous corrective actions against the offending source that is generating the unusual traffic by dropping the packets or limiting it to a "fair share" the number of packets entering the fabric. The work of these agents and the humans tracking network security could be helped if the new generation of routers add information packets that make it easier to detect malicious patterns of use and to track the attacks to their source.

The proposed self healing network will add to the packet handling overhead at each router in the fabric and has the potential to make the system slower, waste bandwidth, and compromise privacy. At first blush, this requirement appears to be impractical, as the Internet is expected to handle trillions of packets every day and would require expensive retrofitting of the existing commercial Internet Service Providers (ISPs). However, such a transition is not only essential to the future economic growth and security of the nation, but also practical given the expected exponential advances in processor, memory, and optical networking technologies. The expected additional overhead in packet handling will be ameliorated by better algorithms, exponential improvements in processor (predicted by Moore's law), memory, and bandwidth technologies and increasing locality of Internet traffic patterns ("Internet is global and the traffic is local").

In addition to the research needed to develop terabit networks, faster routers, efficient algorithms, and distributed computation techniques, research will also be needed for data warehousing of meta-data contained in packet headers, data mining of this data to establish statistical parameters that can be used to classify normal and abnormal traffic requests, and repair strategies for generating a signal (analogous to the busy signal used in voice telephony) to sites making abnormal requests without prior arrangement for surge capacity.

Conclusion

In conclusion, creating a dependable Internet infrastructure that is as dependable as telephone service is essential to the future economic growth and security of the nation. It is possible to create a system capable of achieving these goals while ensuring absolute protection of personal privacy and without major reductions in networking speed. Indeed, rapid advances in computing power and networking speed should make the new security systems nearly invisible to users. The main challenge is to find the right balance between having a dependable Internet infrastructure without compromising the ease of use by non-experts and protecting the privacy of the individuals connected to the infrastructure. To accomplish this will require both new research ideas and the uniform application of known and new ideas across the Internet infrastructure. It makes sense to apply the creative energies of academe to these social problems.

Development of networks capable of meeting our goals for security and privacy will only happen with a concerted research investment supported by both Government and industry. One strategy would be to support a network testbed designed with the specific goal of evaluating innovative strategies for network protection—including commercial concepts. Such a testbed would provide useful networking services and at the same time let commercial operators and Government research organizations evaluate advanced networking security concepts.

It is estimated that market capitalization of Internet based industries created since 1990 is more than a trillion dollars resulting in capital gains taxes of more than $200 billion to the nation. Investing a small fraction of this national income in research towards creating a self healing Internet will ensure the continuation of this engine of growth!

Acknowledgements

This paper has benefited from the comments and suggestions from several PITAC members: Jim Gray, Irving Wladawsky-Berger, Vint Cerf and Bob Kahn and from other colleagues: Anish Arora, V.S. Arunachalam, Ed Lazowska, and Rich Pethia. Please send comments to rr@cmu.edu.

Senator BURNS. Thank you, Doctor. Those are interesting comments.

I am going to move to Senator Abraham, who has joined us now. If you would like to either make your statement or summarize or present it for the record, and if you have questions for this panel, we would entertain those at this time. And then I will followup.

STATEMENT OF HON. SPENCER ABRAHAM, U.S. SENATOR FROM MICHIGAN

Senator ABRAHAM. Thank you very much, Senator Burns. And thank you for your leadership on the Subcommittee level and on the full committee level on these issues. We appreciate what you do on a variety of these key topics.

I just will make a brief statement. I have got two or three conflicting hearings this morning and other events, but I wanted to come by because I think this is a really important topic for us to focus on.

I drew from this panel conclusions similar to ones I reached based on some meetings I had immediately in the wake of the recent spate of hacker activity. I was out in the Bay Area, Silicon Valley, and met with representatives from about 20 companies at that time, which was just in the week afterward, and with a group of businesses in my own State. Although Michigan is not as well-known as a high-tech center perhaps as other parts of the country, we actually do have a real growing industry there. And I came away with conclusions very similar to the ones expressed by the panelists.

I do not think there is any question that we need to proceed in a careful way here. We have to recognize the extent to which Government regulations are going to be effective are limited. I do think that we need to continue to focus on some of the things we can do with respect to penalties that can be invoked against people who commit computer-related crimes. I am not sure the current penalty structure really is adequate based on what I studied.

I think the panels at the current time are kind of low. I think we need to establish Federal and civil criminal penalties against electronic identify theft, attacking one of the tools which is often used by cyber-terrorists and techno-thieves. I think we also need to examine Federal, civil and criminal penalties with respect to unauthorized access to information systems. I think these are areas where we can do some things that do not put such impediments in place that we constrict the development of the Internet and the development of e-commerce activities that are going to be going on.

I also think that we need to encourage Governmentwide policies to improve the security of Federal information systems. That is not so much under our domain in this particular committee, but I think it is an area that we need to, based on these recent developments, that we need to perhaps as a Congress focus more attention on. And I know that Senator Thompson, in his committee, has focused on this and begun to introduce legislation along that line.

And then I also serve on the Judiciary Committee, and we have looked at ways that we could create Federal grant programs to assist State and local law enforcement agencies in deterring, investigating and prosecuting computer crimes. Because obviously some of the resources available at the local level tend to maybe not be adequate to meet some of the challenges that the high-tech criminals pose. And I think that that is a reasonable area for us to both be part of and to look into.

So these are some of the things I am going to be working on. But I think we also have to appreciate that there is sort of, obviously, a need to recognize the proprietary nature of information that is accumulated by industries, of technologies that are developed. And this is where I think some of the comments made in your earlier statements are particularly relevant. We have to appreciate that and understand that we can always come up with, I think, anti-crime legislation that can potentially be effective, but sometimes it

is so effective that it completely inhibits normal human discourse and activity.

I was saying in my meetings in Michigan, we could presumably stop most, if not all, bank robberies if we strip searched everybody who went into a bank. But that probably would mean that very few people went into banks. Similarly, we can probably come up with a variety of processes that would minimize the potential for Internet crime or cyber-terrorism, but at such a level that there would be no more activity of an e-commerce nature or anything else.

We can always overreach. I think we have to be very careful not to. And so I appreciate what you are trying to accomplish today. I look forward to working with you. And I thank the panel. I appreciate very much their participation.

Senator BURNS. Thank you, Senator.

I have just a couple of questions, and then we will just start the dialog. I am concerned. I think Senator Hollings kind of hit on it a while ago, and even the panel on law enforcement or those people who are in charge of monitoring these kind of activities. While I realize that you have got to watch the bottom line—I mean, we are all in business, we have to make a living and we have an obligation to our board of directors and our obligations to our own industry—and given the competitiveness of this industry so far, and we have tried to maintain this to be very open, very competitive, let entrepreneurialship and imagination and ingenuity flow, it seems like we have not really given an extra measure to security until we had this incident happened with this information.

Business and security should be complementary, not mutually exclusive. And I am wondering if you could comment on this. They say you have run out of interest after a while in discussions about security. How can we increase this dialog? And how can we heighten the interest in security and the working between Government and law enforcement?

I want you all to take a shot at this. So, Mr. Misener, if you want to lead it off.

Mr. MISENER. Certainly, Mr. Chairman. There is a need for both locks and police. We spent a lot of time talking about the police today and a little bit recently on the lock side. We at Amazon.com take security very seriously, and it is very important to us as a business and to our customers. As indicated before, we did not experience a break-in at our premises. Rather, it was this surrounding of the premises by this junk traffic that was directed toward our site.

And so, to that extent, to the extent that there was this criminal behavior, we do believe that in addition to the locks that we put on our house, that we also need the police to help enforce against the criminal activity or prosecute the perpetrators of that criminal activity around the outside of the house.

Senator BURNS. Dr. Reddy.

Dr. REDDY. Mr. Chairman, besides the locks and the police, there is a third option. Normally, when we build any infrastructure, whether it is the interstate highway system or anything else, the Government takes responsibility at certain levels. Unfortunately, the Internet fabric, everybody has their own sites and they can secure those, but no one person is responsible for the Internet fabric.

And that is by design. That is the way it was designed in 1969, because we wanted it to be scalable.

However, that particular design has run its course. I think we need new research and new test beds to demonstrate an ultra-dependable network which has all the same features, and it can be shown and it can be used and demonstrated. And that is the responsibility of the Government, in the sense of what Senator Hollings was talking about and what you are also saying. It is not a question of increasing police, or it is not a question of telling private industry to put on more locks. There is another piece in between, the Internet fabric, that no person is responsible for. And therefore, the Government has to take responsibility for it.

Senator BURNS. Mr. Fuhrman.

Mr. FUHRMAN. Thank you, Chairman. If I could add, if we step back a second, everybody looks through their glasses on life and their perspectives are built upon their experiences that they have gone through or others that they have observed. And so I think an unfortunate step that we have taken here at this point is that we have had to wait, in essence, for some of these attacks to occur for folks to wake up and go through the experience and realize that this is now something that they before had either discounted or just had not gotten to yet that is now something to be added up to my priority list.

And I think, as we continue to step closer and we make great progress as we go forward, we are going to see businesses and customers start taking security even more seriously than they have in the past.

Senator BURNS. It is very interesting, the field called biometrics, where users verify their identity through a pad that scans either fingerprints or a monitor that scans retinas, among other devices. Does biometrics have a role to play in increasing security on the Internet in coming years? What is the potential? Anybody can take a shot at that.

Dr. REDDY. Mr. Chairman, biometrics has the same privacy problems. There is even a simpler solution than biometrics. Intel has designed into every chip an I.D. So when a packet is transmitted from a computer, you can add that I.D. But there was a big hue and cry about the privacy issues, and the whole thing stopped dead. Anybody that tries to put biometrics or anything else which involves identification of the individual, as opposed to just the machine that perpetrated the thing, will probably cause the same kinds of issues. So I do not know what the right answer is.

Senator BURNS. Mr. Misener.

Mr. MISENER. Mr. Chairman, I share the assessment that this would cause perhaps a hue and cry if discussed as a viable option, although I would recognize that biometrics and other forms of personal identification are important to protecting actual true security issues as opposed to sort of online e-commerce issues.

Senator BURNS. Mr. Fuhrman, you can comment on this. But I was struck by the fact of what you said a while ago. I really had not thought of it in the context that they did not actually get into your shop, but they surrounded your shop, and prevented anybody else from your normal daily activities. And therein lies the problem, more than the security of gaining entry into your shop.

Is that a correct assessment?

Mr. MISENER. That is correct. But recognize also, sir, that there were security breaches at other sites that allowed the hack attacks to occur. For example, at some universities there were security breaches, true intrusions of their systems, that allowed these distributed denial of service attacks to take place against other systems. And those systems were less well protected than others on the in terms of.

Senator BURNS. It was my understanding that it took several computers to do all this. And if this person that perpetrated this thing, if he had to buy all the computers, he probably would not do it. But he could enter other computers and tell them what to do.

Dr. REDDY. Mr. Chairman, there is a problem here. There is also legal traffic that can demonstrate the same properties as a hacker attack. For example, when Victoria's Secret announced that they were going to have a Web site where they were showing their new fashions, everybody and his brother wanted to see it. And the same denial of service happened there. There is nothing illegal there. It just happened.

It is like what happens when there is an earthquake in California: everybody calls in to make sure that their loved ones are safe. You cannot get through. So it is not just illegal, malicious attacks. Legal things can also cause this problem. That is why you need a self-monitoring, self-healing network, which says, sorry, there is a lot of traffic going, you cannot use it. There is a busy signal.

So some people at least get through, as much as the traffic would permit, at Amazon.com. The rest of the people are not able to get through. Rather than everybody being stopped.

Senator BURNS. The other day I visited a facility that monitors telephone traffic. It tells them where they have a problem, they have a line outage. And it tells them that they are rerouting. And also during particular times of day their traffic is such that there is a potential that they have to add another line or to reroute the traffic or then protect what 911 does and all of this. Are we saying that?

Dr. REDDY. The same thing.

Senator BURNS. The same thing. We are going down the same line.

Dr. REDDY. It is what is called a network management system. We need an Internet network management system. And what happens now is, as we heard from the previous panel, the Government is somehow going to protect each of their sites. But I can still disable people from getting through to your site. And what we need is to stop it at the source, not at the destination. And that requires a complete concept of knowing exactly the overall well-being of the entire network all the time. That is the kind of thing you saw in the telephone systems. We do not have that.

Senator BURNS. Do you envision an automatic thermostat, so to speak?

Dr. REDDY. Yes, that is exactly it. The whole idea is to build a dependable network in which there is a continuous monitoring of the entire traffic from everybody, and knowing where the abnormal

behavior is happening, and then shut them down at the source rather than letting them come all the way to the Government site and there trying to block them from getting in.

Senator BURNS. It offers interesting challenges. It really does. Any closing statements by any of you?

[No response.]

Senator BURNS [continuing]. None at all. Well, we appreciate your coming here today and sharing this information. We will probably investigate this further.

Dr. Reddy, I am very interested in what your testimony is here today, and I would hope that the rest of the Senators on this Committee read it. And I think that they will, because you offer several suggestions in there that I think we should take note of. And all of you who have offered suggestions, I appreciate that.

Again, industry, the teamwork thing has to happen. Because I am not convinced right now that there has to be new laws or anything like that. I am saying that we as an industry have to come together. And it is like I said a while ago, in security, we were all raised that you do not fool around with somebody else's mailbox, but I do not see any warning out there like I saw on a mailbox or our folks got on us about that. I know those things have to be taken into account.

Thank you very much. These hearings are closed.

[Whereupon, at 11:20 a.m., the hearing was adjourned.]

APPENDIX

PREPARED STATEMENT OF MAX CLELAND, U.S. SENATOR FROM GEORGIA

Good morning Mr. Chairman and distinguished guests. The tremendous advances being made in the computer and telecommunications industries are forever changing the way we do business in this country and abroad. This new digital age in which we are living has ushered in the ability to trade stock, shop for a car, buy air line tickets and to buy, sell and trade just about anything else using the Internet. Many of the firms that are engaging in this new way of doing business didn't exist a few years or even months ago. The growth of e-commerce has been so rapid that projections made about how much business will be conducted over the Internet were often outdated as soon as they are published. On March second of this year the Commerce Department released the first ever estimate of retail e-commerce sales or e-tail sales. Reported e-tail sales over the Internet and other electronic networks have reached a historic $5.3 billion in the fourth quarter of 1999.

While there are now new opportunities for the good people of our nation to gain greater productivity and have access to a wider selection of goods and services, there is an attendant menace to on-line businesses which threatens to disrupt the way commerce is conducted over the Internet. This menace is **HACKERs** who are seeking to gain unauthorized access to systems for the purpose of destroying, corrupting, stealing or monitoring information vital to the operation of computer systems owned by others.

These hackers have distinguishing screen names, or aliases, and are apparently very bright, intelligent people with deviant, malicious minds and a hankering for chaos. One suspected hacker is a 17 year-old New England boy who told investigators that he has been using computers since he was three and spends 16 hours a day on the Internet.

All businesses must be protected from the hackers, but no where is it more important than the businesses and industries that are vital to the nation's health, wealth and security and make up our nation's critical infrastructure. These critical infrastructure businesses and industries are engaged in information and communications, banking and finance, basic utilities, aviation, mass transit, public health services, and oil and gas production and storage. On the Government side, the critical infrastructure consists of internal security, Federal law enforcement, foreign intelligence, foreign affairs and national defense. All of these activities must be protected from the destructive, corruptive, stealing or monitoring of information by unauthorized persons. Anyone attempting to hack into these systems must be stopped because their actions threaten our country's security.

A GAO report released March second of this year provides commentary on the proposed Government Information Security Act and cites some very disturbing facts about the state of the Government's computer security:

> The Environmental Protection Agency has had invasions of its systems that resulted in damage and disruption to that agency's operations.
> The Department of Veterans Administration has been cited for weaknesses in its computer systems that could compromise sensitive medical and benefit payment information of our nation's veterans.
> A test on the National Aeronautics and Space Administration's systems reveled that their systems could have been penetrated posing serious threats to orbiting spacecraft and the scientific data received from these spacecrafts.
> The State Department's computers are also vulnerable to attack and unauthorized access by hackers, terrorists or other unauthorized individuals.

It appears that from this listing that there is a pressing need to improve computer security planning and management and to make the cases like these just cited the exception, not the rule in the Government's systems.

Fear, mistrust and the uncertainties created by hackers can slow the economic growth and prosperity that many public and private sector experts envision for the Internet. As the Government sets out to continue to protect our nation's critical in-

frastructure from domestic and foreign intruders and e-businesses set out to reduce the costs of theft and destruction of data and hardware by hackers, we must ensure that people seeking to do business over the Internet are safe from hackers, and that sufficient cooperation and coordination between the Government and private industry is encouraged. Most recently this cooperation resulted in a smooth transition to the year 2000. We can and must replicate these results in the area of computer security.

I am very interested in hearing from the panel about your thoughts with regard to the scope and magnitude of the hacker problem and what your recommendations are for putting hackers out of business.