S. HRG. 106–600

CYBERCRIME

HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON APPROPRIATIONS

UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

SPECIAL HEARING

Printed for the use of the Committee on Appropriations

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

63–940 cc WASHINGTON : 2000

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

COMMITTEE ON APPROPRIATIONS

TED STEVENS, Alaska, *Chairman*

THAD COCHRAN, Mississippi
ARLEN SPECTER, Pennsylvania
PETE V. DOMENICI, New Mexico
CHRISTOPHER S. BOND, Missouri
SLADE GORTON, Washington
MITCH McCONNELL, Kentucky
CONRAD BURNS, Montana
RICHARD C. SHELBY, Alabama
JUDD GREGG, New Hampshire
ROBERT F. BENNETT, Utah
BEN NIGHTHORSE CAMPBELL, Colorado
LARRY CRAIG, Idaho
KAY BAILEY HUTCHISON, Texas
JON KYL, Arizona

ROBERT C. BYRD, West Virginia
DANIEL K. INOUYE, Hawaii
ERNEST F. HOLLINGS, South Carolina
PATRICK J. LEAHY, Vermont
FRANK R. LAUTENBERG, New Jersey
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
HARRY REID, Nevada
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
BYRON L. DORGAN, North Dakota
DIANNE FEINSTEIN, California
RICHARD J. DURBIN, Illinois

STEVEN J. CORTESE, *Staff Director*
LISA SUTHERLAND, *Deputy Staff Director*
JAMES H. ENGLISH, *Minority Staff Director*

SUBCOMMITTEE ON COMMERCE, JUSTICE, AND STATE, THE JUDICIARY, AND RELATED AGENCIES

JUDD GREGG, New Hampshire, *Chairman*

TED STEVENS, Alaska
PETE V. DOMENICI, New Mexico
MITCH McCONNELL, Kentucky
KAY BAILEY HUTCHISON, Texas
BEN NIGHTHORSE CAMPBELL, Colorado

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
FRANK R. LAUTENBERG, New Jersey
BARBARA A. MIKULSKI, Maryland
PATRICK J. LEAHY, Vermont
ROBERT C. BYRD, West Virginia
(ex officio)

Professional Staff
JIM MORHARD
KEVIN LINSKEY
PADDY LINK
DANA QUAM
CLAYTON HEIL
LILA HELMS *(Minority)*
SONIA KING *(Minority)*

CONTENTS

GOVERNMENT PANEL

INDUSTRY PANEL

CYBERCRIME

WEDNESDAY, FEBRUARY 16, 2000

U.S. SENATE,
SUBCOMMITTEE ON COMMERCE, JUSTICE, AND STATE,
THE JUDICIARY, AND RELATED AGENCIES,
COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Judd Gregg (chairman) presiding.

Present: Senators Gregg and Leahy.

GOVERNMENT PANEL

OPENING REMARKS OF SENATOR GREGG

Senator GREGG. Ladies and gentlemen, I will call the hearing to order. Let me thank the Attorney General for her courtesy in coming today and the Director of the FBI for his courtesy on short notice in coming. We also have the Under Secretary of Commerce Bill Reinsch, who depending on the way the hearing goes, we may like to hear from him, also. In fact, I think we probably will. He is a participant.

This hearing is really a continuum of a number of hearings which this committee has had in the area of cybercrime and cyberterrorism. In fact, it was as a result of this committee's efforts that we initiated a fairly significant effort at the suggestion of the FBI and the Justice Department in the area of illegal activity on the Internet involving child pornography and traveler cases. That has also been followed by a very significant effort in this committee, which again was initiated by myself and Senator Hollings and members of the committee, in the area of cyberterrorism, where we have attempted to fund aggressively initiatives within the Justice Department, and the FBI specifically, to try to fight cyberterrorism.

As a result of last week's hacker attacks on major commercial sites, it seemed appropriate to hold a hearing to discuss further what the role of government should be in the area of security on the Internet and protecting the commerce of the country. As a preliminary thought on this matter, it seems to me that we as a government must divide the issue. There are certain functions of activity within the society which are critical to our Nation, certain structures which are essential to our ability to function as a cohesive society, such as our electric grid, our waterworks in our communities, obviously our banking system, and obviously our national defense.

In those areas, the Government has a priority role in making sure that these infrastructure and national defense capabilities are protected and maintained and that the security of those infrastructures are aggressively defended. However, when we get into the area of commercial activity, whether it is selling books or auctioning items, the role of the government, I think, is probably significantly different. That is an area where clearly the commercial community has the first obligation of protecting and securing their sites and making sure that they give their customers the access that they need. And the government's role here must be limited because there is the potential, obviously, for abuse.

But as a corollary to that, the government does have a role, and when a crime occurs, the private sector cannot prosecute a crime. It is a crime to interfere with commerce at a number of different levels and, therefore, the government's participation in protecting the Internet is significant, but as I said, it depends on the area of the Internet, the area of the activity as to the level of government involvement.

So this hearing today is to discuss that second issue primarily of what happens when commercial sites are put at risk because of hacker attacks on those sites. There are a number of areas that I want to go into. First, I hope and suspect we will be getting a report from the FBI and the Attorney General on the status of the present investigation.

Second, we need to know whether or not the Justice Department and the FBI feel there are adequate laws on the books to address the issues which are raised by these questions.

Third, we need to address the question of coordination. By my count, we have at least five or six different major agencies and a number of lesser agencies involved in the issue of cyberactivity and security. We have the Commerce Department and the National Security Council which have been given recently the portfolio by the President to begin a process and in this budget made a budget request for that purpose.

We have the FBI, of course, which has a number of different functions in this area including Computer Analysis Resource Response Teams, the CART teams, which we funded, and the National Infrastructure Protection Center, which again we funded and which there is an additional request for. We have the NIST [National Institute of Standards and Technology] activities, which is an agency of the Commerce Department, which has its own Institute for Information Infrastructure Protection. We have the Defense Department functioning through DARPA [Defense Advanced Research Projects Agency], which has farmed out its activities in this area to the Carnegie Mellon Institute which has up and running a very strong program called CERT, which is a Computer Emergency Response Team.

I learned today in reading the newspaper that the CIA has an initiative. That is the best way to learn what the CIA has as initiatives is to read the newspaper. It being a secret agency, it does not inform us, but we do get to read about it.

So there are obviously a lot of different initiatives in this area. What I am interested in is, where is the coordination? Is there adequate coordination? Is there overlap? If there is overlap, how do we

make sure everybody is working off the same page rather than singing different songs and possibly being off tune?

Fourth, after the coordination issue, we need to address the resource issue. This is a critical issue. It is an issue which this committee has a special attention to. We have tried to address it in the past. This really goes to personnel because we understand that keeping the type of people you need to keep in order to fight the hacker means you are going to have to be hiring people who are extraordinarily highly qualified and who have a tremendous market value.

Now, 2 years ago, this committee recognized that problem and bifurcated the wage and salary system within the FBI so that the FBI had the capacity and has the capacity to go out and hire people who have technology capability at a much higher level of pay than what would have been the traditional reimbursement process. I hope we will find out today whether that is working; whether we can get those folks; whether we do have the resources necessary; and whether we can keep those people in light of the tremendous demand for this type of talent in the private sector. So that is another topic.

That is an outline of what I hope this hearing will go into. Obviously, we would be interested in the initiatives coming from the administration, and we would want to get your thoughts on that also. So having made that statement, I will turn to Senator Leahy. I understand Senator Hollings is not going to be able to make the hearing. Senator Leahy has a great amount of interest in this area and also serves on the Judiciary Committee which has primary authorizing jurisdiction.

Senator LEAHY. Thank you, Mr. Chairman, and I want to commend you for holding this hearing. You and I come from States where we guard our privacy. Well, you ease up on it a little bit every 4 years but the rest of the time, we——

Senator GREGG. But we make mistakes.

Senator LEAHY. And I chuckled when I heard your comment about reading in the paper on the CIA. I give high marks to the current Director for keeping us informed, but I recall a former Director once when in the fourth time in about 2 weeks he came up here to tell us about a matter that he was supposed to notify the Congress about and each time had not and then each time we read about it on the front page of one of the newspapers, and he then showed up to tell us about something that we had first learned about in the papers, and I said to him, Director, I said you really—there is a better way of doing this. Instead of sending somebody up here with all these briefings, just take the New York Times or the Washington Post each day, mark it "Top Secret," and deliver it to us.

I said we get three advantages. One, we will get the information a lot quicker; second, we will get it in far, far greater detail than you have ever given it to us, and three, we get this wonderful New York Times crossword puzzle.

He did not find it as funny as some in the audience today, but, you know, to be serious about this, whether you work in the private sector or in government, you tend to go through all these mazes of security checkpoints. Here in the Senate, for example, you

have the barriers and photo ID cards and metal detectors and X-ray scanners. It is all done to protect us from terrorists or from those who might victimize us by crime. And you find these things now ubiquitous in the private sector, too.

But the irony is every single one of these barriers, these physical barriers, can be circumvented because we have wires coming into this building or any other building. They support the computers and the computer networks that are absolutely necessary. We could not communicate. We could not do our work without them. And to know how easy it is to go past the normal physical barriers—look what happened with the hacker attacks last week on e*trade, ZDnet, Daytime, Yahoo!, eBay, Amazon.com, and a number of sites we saw during the Christmas time with all the sales and the huge spike in e-commerce, but we also know what the Achilles heel would be if this commerce turned out to be vulnerable to outside attack.

In our daily lives, we rely on computers. Director Freeh, you have been to my home in Vermont. You know we are out in the country, and yet here is a place where I do not worry about somebody coming in and stealing things, but I am connected to all my files in my office in Washington. I like being able to work there, but I also like to know there is a certain degree of security. The chairman mentioned CERT, the coordination center. Well, they have provided some very chilling statistics on the vulnerabilities of the Internet and the scope of the problem. Over the last decade the number of reported computer security incidents grew from 6 in 1988 to more than 8,000 in 1999, but that does not reveal the scope of the problem.

According to CERT's most recent annual report, more than 4 million computer hosts were affected by computer security incidents in 1999 alone by damaging computer viruses, names like Melissa or Chernobyl, ExploreZip, by other ways that remote intruders have found to exploit system vulnerabilities. Even before the denial of service attacks last week, CERT documented such incidents grew at a rate of around 50 percent per year which was greater than the growth of the Internet hosts. The Attorney General has visited in Vermont a couple of our law enforcement centers that we use to supply the rest of the Nation, the alien tracking system, and we were so proud when the AG came to visit that. But that has to have security. All of these things—we know that life is changing.

Now I am going after the recess to introduce legislation to broaden the scope of the prohibitions relating to computer hacking, including a refinement of the definition of what constitutes laws and damage caused by an intruder on a computer system. My proposal will contain measures to allow our law enforcement officers to investigate and assist in international hacker cases.

The President has proposed $37 million in additional funding to combat cybercrime in the Department of Justice, $6 million to develop regional computer forensic labs, $11 million to hire 100 more FBI experts, $8 million for U.S. attorneys, and we should look very seriously at that. And last, I will put my whole statement in the record, Mr. Chairman, but I think we ought to listen to one of the best known hackers, now legitimate hacker, in the country, what he said yesterday at the meeting with the President at the White

House. He stated that these massive attacks were something that could have been done several years ago. So we have to assume that there is a whole new generation of ability to attack and get into our computer systems, and I think it is a chilling thing, and so, Mr. Chairman, I am delighted you are having this, and I will stay until I have to get to my other hearing. But I am delighted you are doing it.

[The statement follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

Mr. Chairman, I commend you for your leadership in convening this hearing.

Whether we work in the private sector or in government, we negotiate daily through a variety of security checkpoints designed to protect ourselves from being victimized by crime or targeted by terrorists. For instance, Senate buildings like this one use cement pillars placed at entrances, photo identification cards, metal detectors, x-ray scanners and security guards to protect this physical space.

These security steps and others have become ubiquitous in the private sector as well.

Yet all these physical barriers can be circumvented using the wires that run into every building to support the computers and computer networks that are the mainstay of how we communicate and do business. This plain fact was amply demonstrated by the hacker attacks last week on E-Trade, ZDNet, Datek, Yahoo, eBay, Amazon.com and other Internet sites. These attacks raise serious questions about Internet security—questions that we need to answer to ensure the long-term stability of electronic commerce. More importantly, a well-focused and more malign cyber-attack on the computer networks that support telecommunications, transportation, water supply, banking, electrical power and other critical infrastructure systems could wreak havoc on our national economy or even jeopardize our national defense.

The reports of the CERT Coordination Center (formerly called the "Computer Emergency Response Team"), which was established in 1988 to help the Internet community detect and resolve computer security incidents, provide chilling statistics on the vulnerabilities of the Internet and the scope of the problem. Over the last decade, the number of reported computer security incidents grew from 6 in 1988 to more than 8,000 in 1999. But that alone does not reveal the scope of the problem. According to CERT's most recent annual report, more than four million computer hosts were affected by computer security incidents in 1999 alone by damaging computer viruses, with names like "Melissa," "Chernobyl," "ExploreZip,"and by other ways that remote intruders have found to exploit system vulnerabilities. Even before the "denial-of-service" attacks last week, CERT documented that such incidents "grew at a rate around 50 percent per year" which was "greater than the rate of growth of Internet hosts."

CERT has tracked recent trends in severe hacking incidents on the Internet—both are serious cause for concern. First, hacking techniques are getting more sophisticated. That means law enforcement is going to have to get smarter too, and we need to give them the resources to do this. Second, hackers have "become increasingly difficult to locate and identify." These criminals are operating in many different locations and are using techniques that allow them to operate in "nearly total obscurity."

We have been aware of the vulnerabilities to terrorist attacks of our computer networks for more than a decade. It became clear to me, when I chaired a series of hearings in 1988 and 1989 by the Subcommittee on Technology and the Law in the Judiciary Committee on the subject of high-tech terrorism and the threat of computer viruses, that merely "hardening" our physical space from potential attack would only prompt committed criminals and terrorists to switch tactics and use new technologies to reach vulnerable softer targets, such as our computer systems and other critical infrastructures. The government had a responsibility to work with those in the private sector to assess those vulnerabilities and defend them. That means making sure our law enforcement agencies have the tools they need, but also that the government does not stand in the way of smart technical solutions to defend our computer systems.

Targeting cybercrime with up-to-date criminal laws and tougher law enforcement is only part of the solution. While criminal penalties may deter some computer criminals, these laws usually come into play too late, after the crime has been committed and the injury inflicted. We should keep in mind the adage that the best de-

fense is a good offense. Americans and American firms must be encouraged to take preventive measures to protect their computer information and systems.

That is why, for years, I have advocated and sponsored legislation to encourage the widespread use of strong encryption. Encryption is an important tool in our arsenal to protect the security of our computer information and networks. The Administration made enormous progress last month when it issued new regulations relaxing export controls on strong encryption. Of course, encryption technology cannot be the sole source of protection for our critical computer networks and computer-based infrastructure, but we need to make sure the government is encouraging—and not restraining—the use of strong encryption and other technical solutions to protecting our computer systems.

Congress has responded again and again to help our law enforcement agencies keep up with the challenges of new crimes being executed over computer networks. In 1984, we passed the Computer Fraud and Abuse Act, and its amendments, to criminalize conduct when carried out by means of unauthorized access to a computer. In 1986, we passed the Electronic Communications Privacy Act (ECPA), which I was proud to sponsor, to criminalize tampering with electronic mail systems and remote data processing systems and to protect the privacy of computer users. In the 104th Congress, Senators Kyl, Grassley and I worked together to enact the National Information Infrastructure Protection Act to increase protection under federal criminal law for both government and private computers, and to address an emerging problem of computer-age blackmail in which a criminal threatens to harm or shut down a computer system unless their extortion demands are met.

In this Congress, I have introduced a bill with Senator DeWine, the Computer Crime Enforcement Act, S. 1314, to set up a $25 million grant program within the U.S. Department of Justice for states to tap for improved education, training, enforcement and prosecution of computer crimes. All 50 states have now enacted tough computer crime control laws. These state laws establish a firm groundwork for electronic commerce and Internet security. Unfortunately, too many state and local law enforcement agencies are struggling to afford the high cost of training and equipment necessary for effective enforcement of their state computer crime statutes. Our legislation, the Computer Crime Enforcement Act, would help state and local law enforcement join the fight to combat the worsening threats we face from computer crime.

I am convinced that we should be doing more to combat the current wave of computer crime. Those who are engaged in computer hacking, computer fraud and counterfeiting computer programs should be prosecuted and punished appropriately. As we have seen recently, these kinds of criminals wreak havoc on consumers, our interstate businesses and computer systems. To strengthen our laws in these areas, after the recess I plan to introduce legislation to broaden the scope of the prohibitions relating to computer hacking, including a refinement of the definition of what constitutes loss and damage caused by an intruder on a computer system. My proposal also will contain measures to allow our law enforcement officers to investigate and assist in international hacker cases.

President Clinton has proposed $37 million in additional funding in his fiscal year 2001 Department of Justice budget to combat cybercrime. The President's request includes $6 million to develop regional computer forensic labs, $11 million to hire 100 more FBI experts on computer-related crimes and $8 million for U.S. Attorneys to prosecute cybercrime.

I look forward to working with the Chairman and other concerned Senators to consider this budget request and other steps like our pending legislation to give state and local law enforcement agencies the tools they need to combat computer crime and maintain consumer confidence in electronic commerce.

I am a strong proponent of the Internet and a defender of our constitutional rights to speak freely and to keep private our confidential affairs from either private sector snoops or unreasonable government searches. These principles can be respected at the same time we hold accountable those malicious mischief makers and digital graffiti sprayers, who use computers to damage or destroy the property of others. I have seen Congress react reflexively in the past to address concerns over anti-social behavior on the Internet with legislative proposals that would do more harm than good. A good example of this is the Communications Decency Act, which the Supreme Court declared unconstitutional. We must make sure that our legislative efforts are precisely targeted on stopping destructive acts and that we avoid scattershot proposals that would threaten, rather than foster, electronic commerce and sacrifice, rather than promote, our constitutional rights.

Technology has ushered in a new age filled with unlimited potential for commerce and communications. But the Internet age has also ushered in new challenges for federal, state and local law enforcement officials. Congress and the Administration

need to work together to meet these new challenges while preserving the benefits of our new era. I look forward to hearing from Attorney General Reno and FBI Director Freeh, and the other distinguished witnesses, on this important challenge.

Senator GREGG. Thank you. I appreciate your time, Senator Leahy. Secretary Reinsch, would you like to sit at the table here because I suspect at some point we are going to want to ask you some questions, if you do not mind? I recognize we did not ask you to prepare a statement so I will not ask you to participate.

Mr. REINSCH. I have one.

Senator GREGG. But we would be happy to have your comments at some point. We will start with the Attorney General, however. Appreciate your taking the time to come, Attorney General. Please give us your thoughts, and what we should know, and then we can turn to Director Freeh, and then to Mr. Reinsch, and then we will take questions.

STATEMENT OF HON. JANET RENO, ATTORNEY GENERAL, DEPARTMENT OF JUSTICE

Ms. RENO. Mr. Chairman, Senator Leahy, Mr. Chairman, I have appreciated your thoughtful, constructive support of law enforcement and your leadership in the area of cybertechnology as it is applied to law enforcement. You have a yankee frugality, though, and you have been totally consistent in making sure we spend our monies wisely and according to proper plans, and I personally want to thank you for the contribution you have made to a very effective law enforcement.

Senator Leahy, you are one of the first people that I met as I came to Washington. Your guidance, your wisdom and your thoughts on so many issues relating to matters in the Judiciary Committee have been vital to me, and I thank you so very much.

FEDERAL LAW ENFORCEMENT RESPONSE TO COMPUTER CRIME

As Director Freeh will discuss, computer crime investigators in a number of FBI field offices are investigating the recent computer attacks. They are coordinating the information with the National Infrastructure Protection Center. The agents are working closely with our network of specially trained computer crime prosecutors, who are available around the clock to provide legal advice and obtain whatever court orders are necessary. Attorneys from the CCIPS, which is the Computer Crime and Intellectual Property Section of the Criminal Division, are coordinating with the Assistant United States Attorneys in the field.

Other Federal agencies and the private sector are working with us in a cooperative effort that I think is an example for all of us on how we must work together to address the issue of cybercrime. I am proud of that effort and I am proud of the efforts that have been made to date to ensure investigative and prosecutorial expertise and capacity to address the issue of cybercrime.

There is more to do if we are to be prepared to deal with the challenges in this arena for the future. This is one of my last appearances before this committee. Most of what we say here will not affect me as Attorney General, but it will affect each one of us as citizens of this country. How we deal with cybercrime is one of the most critical issues that law enforcement has ever faced. If we are

successful in our efforts, we will not only protect our citizens from harm, but we will give people confidence in the Internet and in cybertechnology as magnificent tools of commerce, learning and communication.

Mr. Chairman, in the time I have remaining as Attorney General, I would like to work with you and do everything I possibly can to leave for my successors the capacity to ensure the equipment and the expertise necessary to ensure the prompt and professional investigation and prosecution of cybercrime; to make sure that we have the equipment that is sufficiently up to date to deal with the most sophisticated criminals; to immediately and continually eliminate the backlog of computers to be searched, both in the investigation of cybercrime as well as other crimes such as drug crimes.

Also needed are the prevention and deterrence of intrusions or attacks on the Nation's critical infrastructure or other acts of cyberterrorism; and the capacity to detect and trace cybercriminals around the world and bring them to justice. The damage that can be done by somebody sitting halfway around the world is immense. We have got to be able to trace them, and we have made real progress with our discussions with our colleagues in the G–8 and in the Council of Europe.

BUILDING A STRONG PARTNERSHIP

We need to continue to build a strong partnership with State and local law enforcement by which we share expertise, equipment, and avoid costly duplication and fragmentation. 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. We need to develop the means of educating our young people concerning the responsible use of the Internet.

The Department must also address the vulnerability of its own systems. Based on internal reviews, we need enhanced computer security across the Department and we are redirecting our resources and efforts to focus on correcting computer security vulnerabilities. But when threats like the denial of service attacks of last week emerge, we have taken steps and we must continue to do so to protect the Department's computer systems. We must do all we can to reach out to academia and to industry to learn the most up-to-date means of addressing complex technical issues as they emerge in this new exciting and developing world. We must achieve all these goals in a manner that respects and upholds our cherished privacy and our freedoms.

We would like to work with you, Mr. Chairman, and with members of the subcommittee to develop a comprehensive 5-year plan with fiscal year 2001 as our baseline to achieve these results. Recent attacks demonstrate the importance of developing such a long-term coordinated strategy. Mr. Chairman, it was under your leadership that we developed the 5-year plan with respect to counterterrorism. If we focus on cybercrime, and make sure we have the equipment, and the expertise, I think we can do so much and I would like to work with you in that effort.

APPROPRIATIONS NEEDS

In that undertaking, we need your help to refocus resources provided for fiscal year 2000. The level of funding provided in the fiscal year 2000 enacted appropriation for the General Legal Activities (GLA) appropriation is insufficient to cover the base program needs of all the litigating components funded from GLA with the exception of the Civil Rights Division.

For the first time, the Congress allocated specific amounts to each individual GLA component in the report language that accompanies the Appropriations Act. This action made it impossible for me to distribute the appropriated resources as needed. The Criminal Division's allocation was hardest hit of all and this has had serious implications for the Division's ability to support its computer crime efforts. Yesterday, we delivered a reprogramming of resources appropriated to GLA which would make base resource funding available to all the GLA accounts by internally redistributing Congress' allocation of GLA resources and supplementing the total resources available to GLA with funding presently available from the Working Capital Fund unobligated balances.

We need Congress' approval of this reprogramming to ensure the appropriate distribution of the resources among the components and we especially need full base funding restored to the Criminal Division in order to avoid having to reduce Criminal Division staffing by 83 positions including critical positions in the Computer Crime and Intellectual Property Section.

For fiscal year 2001, I am asking for $37 million in funding enhancements to expand the Department's staffing, training and technological capabilities. These enhancements include $4.1 million for 59 new Assistant United States Attorneys and nine additional attorneys in the Criminal Division to prosecute computer and child pornography crimes and to provide guidance to Federal, State and local agencies on effective response to the threat of computer crime; $8.75 million to provide critically needed computer crime investigation and prosecution training to State and local law enforcement agencies; $11.4 million for 100 new FBI computer analysis and response team members. Finally, we intend to enhance law enforcement's ability to deal with evidence available on computers by developing up to 10 new regional computer forensic labs.

Together these enhancements will increase the Department's 2001 funding base for computer crime of $177.6 million by more than 31 percent. If we can work together in these next weeks to develop a plan that addresses these goals, I think it will be extremely important for our future ability to address these concerns. Director Freeh through his strategic plan has begun to address these efforts and we commit to do everything we can to work with you in coming up with something that satisfies your very appropriate concerns and addresses our capacity to leave for my successors an effective effort at the Justice Department.

Senator GREGG. Thank you, Madam Attorney General.

[The statement follows:]

PREPARED STATEMENT OF JANET RENO

Chairman Gregg and other Members of the Subcommittee, I want to thank you for this opportunity to testify on our efforts to combat the growing problem of

cybercrime, particularly in light of the recent denial-of-service attacks on several major Internet sites.

Need for Five-Year Strategy

The recent attacks demonstrate the importance of developing a long-term, coordinated strategy for dealing with cybercrime. The strategy must address the challenges we face, both domestically and abroad, the need for personnel with expertise and the latest cybercrime-fighting equipment, the importance of cooperation and sharing with state and local law enforcement and our international counterparts, the need for educating our young people and others about the responsible use of the Internet, and all of this must be done in a manner that respects and upholds our cherished privacy and freedoms.

Recently, I outlined a 10-point plan that identifies the key areas where we need to develop our cybercrime capability. The key points of this plan 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 need to explore 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.

I would like to work with you, Chairman Gregg, and the Members of the Subcommittee to develop a comprehensive, five-year plan—with fiscal year 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.

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

As Director Freeh will discuss, computer crime investigators in a number of FBI field offices are investigating these attacks. They are coordinating information with the National Infrastructure Protection Center (NIPC). 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. I am proud of the efforts being made in this case, including the assistance we are receiving from a number of federal agencies.

The Challenge of Fighting Cybercrime

The recent attacks highlight some of the challenges we face in combating cybercrime. The challenges come in many forms: technical problems in tracing criminals operating online; resource issues facing federal, state, and local law enforcement in being able to undertake online criminal investigations and obtain evidence stored in computers; and legal deficiencies caused by changes in technology. I will discuss each of these briefly.

As a technical matter, the attacks like the ones we saw last week are easy to carry out and hard to solve. The tools available to launch such attacks are widely available. In addition, too many companies pay inadequate attention to security issues, and are therefore vulnerable to be infiltrated and used as launching pads for this kind of destructive programs. Once the attacks are carried out, it is hard to trace the criminal activity to its source. Criminals can use a variety of methods to hide their tracks, allowing them to operate anonymously or through masked identities. This makes it difficult—and sometimes impossible—to hold the perpetrator criminally accountable.

Even if criminals do not hide identities online, we still might be unable to find them. The design of the Internet and practices relating to retention of information means that it is often difficult to obtain traffic data critical to an investigation. Without information showing which computer was logged onto a network at a particular point in time, the opportunity to determine who was responsible may be lost.

There are other technical challenges, as well, that we must consider. The Internet is a global medium that does not recognize physical and jurisdictional boundaries. A hacker—armed with no more than a computer and modem—can access computers anywhere around the globe. They need no passports and pass no checkpoints as they commit their crimes. While we are working with our counterparts in other countries to develop an international response, we must recognize that not all countries are as concerned about computer threats as we are. Indeed, some countries have weak laws, or no laws, against computer crimes, creating a major obstacle to solving and to prosecuting computer crimes. I am quite concerned that one or more nations will become "safe havens" for cybercriminals.

Resource issues are also critical. We must ensure that law enforcement has an adequate number of prosecutors and agents—assigned to the FBI, to the Department of Justice, to other federal agencies, and to state and local law enforcement—trained in the necessary skills and properly equipped to effectively fight cybercrime, whether it is hacking, fraud, child porn, or other forms.

Finally, legal issues are critical. We are finding that both our substantive laws and procedural tools are not always adequate to keep pace with the rapid changes in technology.

Current Efforts Against Cybercrime

While these challenges are daunting, the Department has accomplished much in building the infrastructure to combat cybercrime. Director Freeh will discuss the work of the NIPC and the Computer Crime Squads established around the country. Similarly, in the Department, we have a cadre of trained prosecutors, 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 Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and was elevated into a Section in 1996. With the help of this Subcommittee, CCIPS has grown from five attorneys in January of 1996, to eighteen attorneys today. CCIPS works closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators" (CTCs) in U.S. Attorney's Offices around the country. Each CTC is given special training and equipment, and serves as the district's expert in computer crime cases.

The responsibility and accomplishments of CCIPS and the CTC program include:

Litigating Cases:

CCIPS attorneys have litigating responsibilities, taking a lead role in some computer crime and intellectual property investigations, and a coordinating role in many national investigations, such as the denial of service investigation that is ongoing currently. As law enforcement matures into the Information Age, CCIPS is a central point of contact for investigators and prosecutors who confront investigative problems with emerging technologies. This year, CCIPS assisted with wiretaps over computer networks, as well as traps and traces that require agents to segregate Internet headers from the content of the packet. CCIPS has also coordinated an interagency working group consisting of all the federal law enforcement agencies,

which developed guidance for law enforcement agents and prosecutors on the many problems of law, jurisdiction, and policy that arise in the online environment.

Working with the U.S. Attorney's Office in the District of New Jersey and the FBI, as well as with state prosecutors and investigators, CCIPS attorneys helped ensure that David Smith, the creator of the Melissa virus, pled guilty to a violation of the computer fraud statute and admitted to causing damages in excess of $80 million.

CCIPS is also a key component in enforcing the "Economic Espionage Act," enacted in 1996 to deter and punish the theft of valuable trade secrets. CCIPS coordinates approval for all the charges under the theft of trade secret provision of this Act, and CCIPS attorneys successfully tried the first jury case ever under the Act, culminating in guilty verdicts against a company, its Chief Executive Officer, and another employee.

The CTCs have been responsible for the prosecution of computer crimes across the country, including the prosecution of the notorious hacker, Kevin Mitnick, in Los Angeles, the prosecution of the hacker group "Global Hell" in Dallas, and the prosecution of White House web page hacker, Eric Burns, in Alexandria, Virginia.

Training

CCIPS has spearheaded efforts to train local, state, and federal agents and prosecutors on the laws governing cybercrime, and last year alone gave over 200 presentations to a wide variety of audiences. In addition, CTCs across the country are training prosecutors and agents in their districts in a variety of fora.

CCIPS also chairs the National Cybercrime Training Partnership (NCTP), a ground-breaking consortium of federal, state, and local entities dedicated to improving the technical competence of law enforcement in the information age. The NCTP has made great strides in creating a comprehensive prototype training curriculum for agents and prosecutors in a full range of infotech topics.

International

The borderless nature of computer crime requires a large role for CCIPS in international negotiations. CCIPS chairs the G–8 Subgroup on High-tech Crime, which has established a 24 hours a day/7 days a week point of contact with 15 countries for mutual assistance in computer crime. CCIPS also plays a leadership role in the Council of Europe Experts' Committee on Cybercrime, and in a new cybercrime project at the Organization of American States.

Infrastructure Protection, Policy and Legislation

CCIPS provided expert legal and technical instruction and advice for exercises and seminars to senior personnel on information warfare, infrastructure protection, and other topics for the Department of Defense, the National Security Agency, the Central Intelligence Agency, and others. Further, the Naval War College invited CCIPS to give a featured presentation at a high-level, invitation-only conference on cyberwarfare and international law. CCIPS also led the Department's efforts to counter cyberterrorism through its work on PDD–63, the Five-Year Counterterrorism Strategy, its support to the National Infrastructure Protection Center.

CCIPS works on a number of policy issues raised at the intersection of law and technology. CCIPS attorneys meet regularly with a number of industry groups to discuss issues of common concerns, and helped establish the Cybercitizen Partnership in cooperation with high-tech industries to help identify industry expertise which may be needed in a complex investigation, to initiate personnel exchanges and to help safeguard our children.

CCIPS attorneys propose and comment on legislation that affects their high-tech mission.

Other Sections of the Criminal Division—including the Fraud Section, the Child Exploitation and Obscenity Section, and the Terrorism and Violent Crime Section—are responding as crimes within their areas of expertise move online.

Overall, the Department has the prosecutorial infrastructure in place to combat cybercrime. We need the resources to keep the program growing to keep pace with the growing problem.

Additional Resources and Tools Are Needed

We appreciate the Subcommittee's support for many of the efforts described above, but I also need your help to refocus resources provided for fiscal year 2000. The level of funding provided in the fiscal year 2000 enacted appropriation for the General Legal Activities (GLA) appropriation is insufficient to cover the base program needs of all the litigating components funded from GLA, with the exception of the Civil Rights Division. In particular, the specific amounts provided to the Criminal

Division's has serious implications for the Division's ability to support its computer crime efforts.

Yesterday, we submitted a request to reprogram resources appropriated to GLA which would make base resource funding available to all the GLA accounts.

We especially need full base funding restored to the Criminal Division in order to avoid a reduction in Criminal Division staffing by 83 positions, including critical positions in the Computer Crime and Intellectual Property Section.

We must have prosecutors, both in the field and here, in Washington, to deal with cybercrime investigations.

The Division has shifted more of its resources than ever to combat cybercrime. Attorneys in the Fraud Section are now focusing on internet fraud cases, attorneys in the Child Exploitation and Obscenity Section are doing more to combat on-line child pornography. We simply cannot support the demand for more anti-cybercrime positions at our current funding level.

For fiscal year 2001, I am asking for $37 million in funding enhancements to expand he Department's staffing, training and technological capabilities to continue the fight against computer crime. These enhancements include:

—$4.1 million for 59 new Assistant U.S. Attorneys and 9 additional attorneys in the Criminal Division to prosecute computer and child pornography crimes, and to provide guidance to federal, state and local agencies on effective responses to the threat of computer crime.

—$8.75 million to provide critically needed computer crime investigation and prosecution training to state and local law enforcement agencies.

—$11.4 million for 100 new FBI Computer Analysis and Response Team (CART) members who will be dispatched to support investigations into computer related crimes, as well as expanding the use of the Automated Computer Examination System, which aids in computer forensics examinations.

—Finally, we intend to enhance law enforcement's ability to deal with evidence available on computers by developing up to 10 new Regional Computer Forensic Labs.

Together, these enhancements will increase the Department's 2001 funding base for computer crime of $177.6 million, 31 percent more than in 2000.

We also need to consider additional tools to locate and identify cybercriminals. For example, we may need to strengthen the Computer Fraud and Abuse Act by closing a loophole that allows computer hackers who have caused a large amount of damage to a network of computers to escape punishment if no individual computer sustained over $5,000 worth of damage. We may also need to update our trap and trace laws, under which we are able to identify the origin and destination of telephone calls and computer messages. Under current law, in some instances we must obtain court orders in multiple jurisdictions to trace a single communication. It might be extremely helpful, for instance, to provide nationwide effect for trap and trace orders.

We must also ensure that in upgrading our computer-crime fighting laws, we ensure that appropriate privacy safeguards are maintained and, where possible, strengthened. For example, recent investigations have revealed serious violations of privacy by hackers, who have obtained individual's personal data, such as credit cards and passwords. An increase in the penalty for violations of invasions into private stored communications may be appropriate. We would like to work with Congress to develop a thoughtful and effective package of tools that allow us to keep pace with cybercriminals, update the laws that allow us to locate and identify cybercriminals, and ensure that privacy safeguards are respected and, where possible, strengthened.

Finally, I believe one important answer lies in educating our youth and others in society, that computer hacking is not only illegal, but ethically wrong. Most of us know that we should not break into a neighbor's house or read his mail, but many have not applied these same values to their online activities. Last April, I announced that the Department, along with the Information Technology Association of America had formed the Cybercitizen Partnership, a national campaign to educate and raise awareness of computer responsibility. We hope the Partnership will announce a nationwide public awareness and education campaign in the near future.

I look forward to working with the Subcommittee to ensure we have a robust and effective long-term strategy for combating cybercrime, protecting our nation's infrastructure, and ensuring that the Internet reaches its full potential for expanding communications, facilitating commerce, and bringing countless other benefits to our society.

STATEMENT OF HON. LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE

Senator GREGG. Director Freeh.

Mr. FREEH. Thank you, Mr. Chairman, Senator Leahy, Attorney General Reno. Let me just echo the Attorney General's appreciation on behalf of the FBI and I think the entire national law enforcement community to you, Chairman Gregg, Senator Hollings, and particularly to this committee, for what has really been a consistent and now long-standing support in the area of technology crimes and the ability for law enforcement agencies—State, local and Federal—to deal with these issues.

I recall in 1997, you chaired a hearing together with Chairman Stevens, and for the first time, at least in our memory, a committee here addressed not just the immediate issues with respect to counterterrorism threats and the cyberterrorism implications of those threats, but looked for the first time to developing a long-term planning and asset evaluation and resource allocation plan. That plan has developed and prospered.

Senator Leahy, let me take the opportunity to thank you also for the support that you have shown in this area, back in 1994, leading the efforts in the Senate on the Communications to Law Enforcement Assistance Act. An act which you recall some people in town said could never be passed, was passed and gave not just the Federal Government but the State and local police forces around the country the continued ability, not any new powers, but the continued ability to exercise court-ordered electronic surveillance without changing the balance of the Fourth Amendment, and really getting into the information age with respect to our technical ability. So let me just begin by thanking you and thanking the Attorney General for her valued support and continuous support in the area of technical assistance to law enforcement.

NEED FOR COOPERATION

Going beyond 1997 when you inaugurated these hearings, Chairman Gregg, there is no doubt anymore that these are issues which are critically important to the success of law enforcement. Looking at Judge Webster's report just a few weeks ago, the Commission on the Advancement of Law Enforcement, which is a congressionally required commission, he says, among other things, global crime, cybercrime and terrorism pose the new emerging security threats to the Nation and challenge the Federal law enforcement community.

The report talks about not only the importance of resource allocation but also coordination, which is the issue that you highlighted, and perhaps just as importantly the cooperation and input from the private sector. Like any other area of the government, the FBI, State and local police departments, and prosecuting authorities cannot deal with this issue without the cooperation and assistance of the private sector, particularly in the type of cases that I will talk about in a moment. These companies are not only victims of some of these crimes, but have uniquely the resident expertise to furnish not only the investigative support and tools that are necessary, but also, indeed in many cases, the insight into their own systems.

I am very pleased to say that not just as a result of the National Infrastructure Protection Center, which this committee authorized and set up, and the use of our investigators throughout the course of the last couple of weeks, the assistance from the private sector has been extraordinary. Not just the victim companies but dozens of other companies, scientific experts, academic scholars, think tanks, associations have called the FBI and gave in many cases not just valuable leads but support, ideas, and in some cases technology assistance to pursue what has been a very complex and fast-moving investigation. This one would never get out of the starting gate without the current structures as you have authorized them and more importantly the interoperability of that structure with not only other Federal, State, and local enforcement agencies and the private sector itself.

CHANGING TECHNOLOGY CHALLENGES

You know if I came in one morning and said we were faced with the invention of the automobile, the telephone, and the radio, and that law enforcement needed your assistance to deal with this new technology, we would sit down and look at vast array of resources that would be necessary to deal with this technology being used in part by people who would commit crimes. In many ways, the situation beginning several years ago is a comparable situation, although because the technology is now not only more complex but in some cases changes on an 18 month cycle, perhaps even a greater challenge.

And as we would, we would have to respond to that threat, devise resources, plans and infrastructure to make sure that law enforcement had the continued capacity to do its traditional role of protecting the people we serve, but doing it not only in the face of the challenge of these technologies, but also using those technologies. In fact, that is what the Congress has done over the last couple of years. The structures that I will speak about briefly in a moment are really the direct result and the absolute minimum ingredient required to deal with these issues.

DENIAL OF SERVICE CASES

With respect to the current investigation, I will give you a quick synopsis of it. Obviously, there are aspects of it that I cannot go into because of the nature of the case and the fact that criminal prosecutions may very well result. Going back several months to the fall of last year, we at the FBI began to receive reports about a threat to the Internet from the distributed denial of service attacks, which is what was evidenced over the last couple of weeks. In these types of attacks, hackers first break into the computer system of an unwitting victim and then plant what they call malicious programs. They go by names such as Trinoo, Tribal Flood Net, Stacheldraht. Planting the malicious systems on unsuspecting or unwitting computer hosts is the first step in the line of that attack. This can be done hours, days, weeks, or even months before the actual attack occurs.

The hacker then sends a command that would activate the program which results in the victim computer systems themselves sending repeated messages against a target system which is what

happened in these cases. In some instances, the malicious program includes an embedded start date and time in its code precluding even the need for a separate activation command.

Because the hacker uses a "spoofed" or non-valid Internet address, the target system overloads because the target system is unable to confirm the receipt of the messages from the computer sending that message. As a result, the build up of unconfirmed messages overwhelms these target systems which in turn denies legitimate access by the regular users.

In December 1999, again with notice of some of these threats, the National Infrastructure Protection Center, which as I noted has only been in existence since December 9, 1998, issued an alert to the community regarding these threats. In fact, for the first time, NIPC made available to the industry a software tool that can be used to detect the presence of service coding. This is the first time that this was done. This tool was downloaded, we know, by hundreds and hundreds of users and, hopefully, put to some good use with respect to both detection and the furnishing of subsequent leads.

On February 8, we received reports that the Yahoo! site had experienced the first coordinated denial of service attack. The days that followed, as reflected in your display here in the hearing room, Amazon.com, eBay, e*Trade, and CNN.com also reported similar denial of service outages. The victim companies of these attacks, as I mentioned, are cooperating fully with the FBI and, as I mentioned, in many cases furnishing, in addition to leads, very important technical support. Additionally, members of the community at large, in fact, some hackers, many of whom condemned the present attacks publicly, have come forward and supplied extremely valuable information to the FBI for which we are very grateful.

Five of our major offices where the target companies are located, Los Angeles, San Francisco, Atlanta, Boston, and Seattle, have initiated full investigations. Seven secondary offices are working in primary support of those offices. In addition, all of our divisions and many of our overseas offices, as I will note in a moment, are furnishing active support in this very fast-moving investigation.

Analysts and computer scientists, both within the NIPC as well as outside, are reviewing and analyzing voluminous material from the target companies logs which have been furnished. This is a very time consuming procedure. The investigation is continuing and even public reports this morning, accurately reflect an investigation which is now stretching literally around the world, working with our overseas FBI offices in places like Canada, Germany, and several other countries, and working with our liaison police partner services in many of these countries running down leads, interviewing people, asking for technical records as well as assistance. This is the nature of these investigations.

As we saw over the millennial period, the ability to conduct investigations in this particular subject matter requires absolutely the instantaneous ability to contact and work with our overseas partners, which is why, thanks to the support of this committee and other committees, the FBI now has 35 foreign Legal attaché offices. We had 21 in 1993. These offices give us the ability to literally pick up the phone and have an FBI agent familiar with the

case walk into the host law enforcement agency and receive law enforcement assistance that could never otherwise have been received in that kind of a time frame. We are very, very thankful for that assistance.

We have been very, very pleased with the progress of the investigation. There are fast developing leads as we speak and, hopefully, we will be able to report with more details in the coming days and weeks.

CYBERCRIME AND COMPUTER INTRUSION THREATS

I would like to just talk a little bit about the emerging cybercrime and computer intrusion threats. We know that the growth of the Internet has certainly been the single reason why these threats have been not only elevated but why the compromising of the systems that we have seen in the past few weeks has such broad implications.

Last year, 1999, there were over 100 million Internet users in the United States. By 2003, experts project the number of users to reach 177 million in the United States and over 500 million worldwide. Economic commerce, a significant new sector of our economy, accounted in 1999 for about $100 billion in sales over the Internet. By 2003, electronic commerce is projected to account for sales in excess of $1 trillion. And the rate of growth after that will clearly be exponential.

Over the past several years, we have seen and investigated a range of computer crimes and threats really across the spectrum. And I want to just briefly refer to some of those. There are the insider threats that computer systems within universities, within corporations, and even within government entities have experienced. A 1999 Computer Security Institute report indicated that 55 percent of the respondents had reported malicious activity from insiders with respect to their individual entities or corporations.

Another brand of these attacks and threats are in the area of hackers about which we have seen much activity. There is a subcategory which we referred to as "hacktivism," which are politically motivated attacks. We saw that during the recent hostilities in the former Yugoslavia with hundreds and hundreds of threats and computer attacks being launched against NATO web servers as well as institutions in many of the NATO countries. There are the virus writers, which is a particularly dangerous type of threat. Back in 1999, the FBI in conjunction with some State and local partners, particularly the New Jersey State Police, solved the Melissa Macro Virus case. If you recall, and again, very importantly for purposes of liaison with the private sector, the New Jersey State Police received some information from America Online that came to the FBI in our Newark office where we have one of our computer squads. A series of investigations were conducted jointly which resulted in several searches and arrests. The individual who pled guilty admitted to activities which affected over one million computer systems and caused over $80 million worth of damage.

Another brand of these threats represent activities by organized criminal groups. In another case last year, two members of a group who called themselves the "Phonemasters" were convicted of the theft and possession of unauthorized access devices. This was a

case where the subjects penetrated MCI, Sprint, AT&T, and Equifax. We needed and obtained judicially approved surveillance orders to conduct the investigation using intercept technologies which were very, very complex and had to be tailor made to use in those particular cases. To give you some idea of the scope of the plan, the individuals downloaded thousands of Sprint calling cards. Some of these were sold to a Canadian citizen. He in turn passed them to a citizen back in Ohio. This was all done by computer. They were then sent to an individual in Switzerland and they ended up in part in the hands of some organized crime groups down in Italy. This is typical in many respects with regard to this type of criminal activity.

We have another category called the distributed denial of service attacks which we have talked about this morning. We also see threats and attacks involving economic espionage. The economic espionage statute, which the Congress passed in 1996, was particularly designed to deal with the theft by computer of valuable trade secrets, where losses of billions and billions of dollars can occur according to the American Society of Industrial Security.

INNOCENT IMAGES

We have another broad set of criminal activity being conducted by individuals, and perhaps the one most notoriously known, and certainly you have been the principal source of the enforcement resources that have been used in this area, named Innocent Images cases. These are cases where pedophiles use the technology of the Internet to go into people's homes to contact minors, to make arrangements to see them, which often requires traveling interstate. We opened 1,497 of these new cases last year, fiscal year 1999. We have made 193 arrests, and obtained over 108 convictions. This is an activity which is now being worked not only by the FBI, but again because of your support and the committee's support, it is being worked in a coordinated fashion by many State and local agencies in cooperation with the FBI.

TERRORIST AND FOREIGN THREATS STRATEGY

We also have other threats that come not from individuals and not even from within the United States but from terrorists, from foreign intelligence services. The whole subject matter of information warfare, of course, gets into national security issues well beyond the purview of the FBI. But the scope of threats on the front of cyberspace and cybercrime; as shown just by this very brief summary, is obviously an immense one.

CYBERCRIME FIGHTING STRATEGIES

I think there are probably some keys and some experience that we have shown relevant directly to our success in any crime fighting strategy involving cybercrime and cyberspace. I would like to highlight just a few of these. The first one is law enforcement investigative capacities. The second one is building prosecutorial expertise—the Attorney General referred to that in part. Third, developing partnerships with industry and academia—these are absolutely vital if we are to be successful. Fourth, building law enforce-

ment data forensic and technology capabilities. Again, these can be built without disturbing the balance of the Fourth Amendment, without people worrying about the government operating national computer systems. These can be done under our existing Constitution and enabling statutes. And finally, the issue of encouraging not only computer ethics but the lawfulness of computer use and computer law, particularly in the area of law enforcement.

NATIONAL INFRASTRUCTURE PROTECTION CENTER

With respect to building law enforcement investigative capabilities, this obviously is the vital and first building block. We are, as I said, grateful for your support and your leadership in the establishment of the National Infrastructure Protection Center. This center, as you know, is unique. It is the only national organization devoted to investigation, analysis, warning and response to attacks against our infrastructure. It was established in December 1998. There are 193 FBI special agents around the field who are particularly qualified and who reside in the investigative part of this program. There are over 100 personnel back here at headquarters in NIPC. Many other government agencies have representatives there.

The private sector has representation there. We have State and local participation. We even have participation from some of the national security agencies. In all we have 16 NIPC squads around the United States. Again, these are recently established and five of them are working on the main cases that I have mentioned before. They share much of their information with State and local partners. We use a series of Federal channels for sharing information including Law Enforcement On-Line and the national law enforcement telecommunications system. We have a key asset program managed by this activity which identifies those key assets in infrastructure which could be compromised.

We have an InfraGard program, which is a program that directly involves the private sector in the planning as well as the reaction to some of these attacks. We have a 24 hour watch system at our FBI Headquarters which monitors not just threats but in some cases, as I mentioned, becomes the originating point for intelligence as it is collected and enables us to take preventive action as we tried to do earlier last year.

One of the issues that you mentioned that I would just like to respond to is the hiring, training, and retention of the people who are necessary to perform this work. And that has been a continuing challenge and will probably be our foremost personnel challenge in the years to come. We were very pleased several years ago when the Congress provided the FBI with a pilot program to use our Title 5 exemption authority to hire people who could not otherwise be hired because their talent and the competition for their work is such that the usual GS pay scale would be insufficient to attract and retain them.

We have been able to staff over 54 experts, particularly in scientific and computer positions, under this program. We would very, very much like to extend the authority for that program which is due to expire in September of this year. My prediction is that if that program is extended and we continue to use it and expand it,

we will have the ability to do exactly what you would like us to do and what the American people would like us to do: get the men and women into the FBI, not just the agents, but the analysts, the computer scientists, the people who understand these codes, and make sure that we are able to keep them. The training and expertise that they bring is also made available to our State and local partners.

One of the other major functions of the NIPC is training and liaison. We have trained hundreds of State and local officers, other Federal officers, in the area of computer crimes. We have even given them, in many cases, some of the tools and techniques necessary to perform this job. But the personnel and the authority to hire over and above the current GS scale is absolutely vital for us.

INTERNATIONAL COOPERATION

I also want to mention again how critical it is that we have not only the domestic law enforcement network and liaison but the international one. There is no computer hacking case of any large dimension that I can imagine where it is not likely to have leads, evidence, witnesses, and needs that go well beyond the United States to literally places around the world. Over the millennium weekend, we did exactly that. It was primarily in the counterterrorism area, but we had agents and computer forensic experts literally around the world working with our liaison partners because that is the nature of this venue and that is where these cases very, very quickly take us.

We have the need obviously, as the Attorney General mentioned, to continue to obtain necessary equipment, including basic hardware to do our job. The 2001 request asks for an additional $40 million for the Information Sharing Initiative. That is the initiative that buys basic hardware and computers to be used by our agents and other personnel to conduct these investigations. We are hoping to receive the final approvals to spend the $80 million which the Congress has authorized and appropriated in the fiscal year 1999 and 2000 budgets and we are hoping to get the final paperwork up to the committees within the next couple of weeks.

BUILDING PROSECUTORIAL EXPERTS

The second broader area that I mentioned is building prosecutorial expertise. The best computer analysts and the best technical agents in the world will not succeed at the end of the day unless there are trained prosecutors with the ability, the know-how, and the experience to assist in the complex investigation of these cases where many legal issues, including privacy issues and Fourth Amendment issues, take different permutations, arise and have to be addressed very speedily and decisively. We are very thankful to the Attorney General for her strong support and leadership in the Department for the development of a strong cadre of Assistant U.S. Attorneys who are able to do these cases and respond to them as the needs arise.

PARTNERSHIP WITH INDUSTRY AND ACADEMIA

The other area I have alluded to several times, the partnerships with industry as well as academia. Yesterday, the head of my laboratory, Dr. Kerr, met with the head of the Thayer School of Engineering to discuss direct FBI participation in the Thayer School Institute for Security Technology Studies, which addresses among other things the primary area of cybersecurity. This is the type of support that we desperately need not only to pursue investigations but also to develop tools and techniques that can be used in these cases to do research and development—which our investigators who are very busy do not always have the time and luxury to do, and which is particularly suited for academia as well as the private sector.

BUILDING FORENSIC AND TECHNICAL CAPABILITIES

The other area—building forensic and technical capabilities is something where I think we have made a very good start. We have 142 full- or part-time CART examiners. These are the individuals who do the forensic examinations, who can take evidence off a hard drive that even the people who are fairly sophisticated think has been erased and deleted from the system. This is a demand which is growing exponentially. We had about 1,800 examinations in the last year. We predict by the end of next year, there will be 6,000 of these examinations required on a yearly basis. Some of the cases, because of their complexity and because of the growth of the capacity of hard drives, require more and more time, more and more complex analysis and techniques.

In 1998, most of the computers that were sold had hard drives with a six to eight gigabyte capacity. By the end of this year, we are going to see 60 to 80 gigabyte capacities. What this means is that you double, double, and double again the magnetic area that needs to be searched to obtain evidence as well as for other preemptory examinations. What this means is that the capacity to do more electronic type of examinations will be required. We have a system that the CART examiners use and which this committee has funded called the ACES system, which is the Automated Computer Examination System. We have asked in the current budget proposal for a continuation of that funding. ACES allows the examiners to expeditiously look at huge areas of media which otherwise even under technical means would take an enormous amount of time. In some cases, not these cases, but others where lives may literally be at risk, this time consumption is very, very critical.

We need to propagate and decentralize the computer examining abilities that we have in the FBI. This goes along the lines you alluded to before about encouraging and supporting State and local expertise. One very successful effort in this area was the recent establishment by the FBI and State and local authorities in San Diego, California, of a regional computer forensic lab, the first time that we have undertaken this type of a joint venture. What this does is establish a regional laboratory for computer examinations so the investigators, particularly State and local investigators in that area, do not have to rely on our headquarters facilities or even FBI stand alone capacity to conduct these examinations.

This creates a center of excellence. It is a method to enhance training as well as other expertise. We are looking at doing the same type of establishments in the New England area, and in the Dallas area. The cost of these start-ups is very minimal and the return and the benefit—not just to the State and local authorities but the ability to cut some of the backlogs coming back to Washington and the attendant delays—we think is a very, very good formula for success.

So we want to look at this very carefully. We want to make sure the results are as impressive as they have been so far. This is an area where I think very critically we need to get this technology and law enforcement ability out to our State and local partners.

COUNTERENCRYPTION

I wanted to mention a little bit about some of the other engineering issues. I mentioned the ACES system. I referred earlier to the Communications Assistance for Law Enforcement Act, the CART examinations. We also need again the ability to work these cases not only in a digital environment as we find ourselves but an encrypted environment. We are finding more and more, 53 new cases last year, computer media as well as stored data, where encryption has made the information and the potential evidence all but worthless or unavailable to us because we do not have the plain text and there is no ability to understand, either on a real time basis or historical basis, what it is that is being discussed by the hackers, what plans reside in their encrypted files, and all the other impediments that this poses.

This is a huge issue not just for law enforcement in general but particularly in the area of computer crime and cybersecurity. Without the ability for law enforcement officers to get court-ordered access to plain text, we are going to be out of business in a large number of these cases. We will never know in some cases who the subjects are, what the conspiracy consisted of, what the objectives were. We will be operating with basically primitive tools in a very high tech environment.

This committee has held hearings on this before. You have certainly supported our budget requests in trying to address this area. As I have testified to numerous times over the last 7 years, if this area remains unaddressed, not just for the FBI but for our State and local partners, we will be very, very much unable and incapable of investigating some of these major cases. As we have testified before, we do not need a change in the Constitution or our statutory authority to do this. We can obtain plain text access which comes only with a court order without changing any of the parameters and without changing the statutes that legitimately protect not just privacy but the expectation of privacy. But if it is unaddressed, we are not going to be able to work in many of these cases.

DEVELOPING COMPUTER ETHICS

The last area that I just wanted to mention briefly is encouraging the development of computer law in the law enforcement area, as well as computer ethics. I think that is a theme that has to become much more conversant in our universities, our schools,

our workplaces, our Government places. We have to respond to some of these incidents, even the ones that are non-criminal, with a framework of law as well as an ethical framework that seeks to deter and discourage activities that affect these systems and promote the positive side of it.

Again, I am very, very pleased to be here and on behalf of the law enforcement community—and I emphasize the State and local community. I want to thank this committee, Mr. Chairman, for your leadership in this area. We have made a good start. We have found in the last couple of weeks that although we were busy, we were not overwhelmed. We have been able to follow leads. The response and support from the other government agencies and the private sector has been enormous. So we are in the ballgame right now thanks to your support, and the resources we have received. We want to make sure that balance does not change in the next couple of years. Thank you.

[The statement follows:]

PREPARED STATEMENT OF LOUIS J. FREEH

Good morning, Mr. Chairman and members of the Subcommittee. I am privileged to join Attorney General Reno in this opportunity to discuss cybercrime—one of the fastest evolving areas of criminal behavior and a significant threat to our national and economic security.

Twelve years ago the "Morris Worm" paralyzed half of the Internet, yet so few of us were connected at that time that the impact on our society was minimal. Since then, the Internet has grown from a tool primarily in the realm of academia and the defense/intelligence communities, to a global electronic network that touches nearly every aspect of everyday life at the workplace and in our homes. 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. The recent denial of service attacks on leading elements of the electronic economic sector, including Yahoo!, Amazon.com, Ebay, E*Trade, and others, had dramatic and immediate impact on many Americans.

I would like to acknowledge the strong support this Subcommittee has provided to the FBI over the past several years for fighting cybercrime. This Subcommittee was the first to support resources—back in fiscal year 1997—for establishing a computer intrusion investigative capability within the FBI. You have generously provided support for our efforts against on-line sexual exploitation of children and child pornography—the Innocent Images initiative, as well as to develop our Computer Analysis Response Team (CART) program, and the creation of computer crime squads in our field offices. For that support, I would like to say thank you.

In my testimony today, I would like to first discuss the nature of the threat that is posed from cybercrime and then describe the FBI's current capabilities for fighting cybercrime. Finally, I would like to close by discussing several of the challenges that cybercrime and technology present for law enforcement.

CYBERCRIME THREATS FACED BY LAW ENFORCEMENT

Before discussing the FBI's programs and requirements with respect to cybercrime, let me take a few minutes to discuss the dimensions of the problem. Our case load is increasing dramatically. In fiscal year 1998, we opened 547 computer intrusion cases; in fiscal year 1999, that had jumped to 1,154. At the same time, because of the opening the National Infrastructure Protection Center (NIPC) in February 1998, and our improving ability to fight cyber crime, we closed more cases. In fiscal year 1998, we closed 399 intrusion cases, and in fiscal year 1999, we closed 912 such cases. However, given the exponential increase in the number of cases opened, cited above, our actual number of pending cases has increased by 39 percent, from 601 at the end of fiscal year 1998, to 834 at the end of fiscal year 1999. In short, even though we have markedly improved our capabilities to fight cyber intrusions, the problem is growing even faster and thus we are falling further behind.

These figures do not even include other types of crimes committed by a computer such as Internet fraud or child pornography on-line.

As part of our efforts to counter the mounting cyber threat, the FBI uses both full National Infrastructure Protection and Computer Intrusion squads located in 16 field offices and is developing baseline computer intrusion team capabilities in non-squad field offices. Further, we are establishing partnerships with state and local law enforcement through cybercrime task forces.

Cyber Threats Facing the United States

The numbers above do not provide a sense of the wide range in the types of cases we see. Over the past several years we have seen a range of computer crimes ranging from simple hacking by juveniles to sophisticated intrusions that we suspect may be sponsored by foreign powers, and everything in between. A website hack that takes an e-commerce site off-line or deprives a citizen of information about the workings of her government or important government services she needs, these are serious matters. An intrusion that results in the theft of credit card numbers or proprietary information or the loss of sensitive government information can threaten our national security and undermine confidence in e-commerce. A denial-of-service attack that can knock e-commerce sites off-line, as we've seen over the last week, can have significant consequences, not only for victim companies, but also for consumers and the economy as a whole. Because of these implications, it is critical that we have in place the programs and resources to confront this threat. The following is a breakdown of types of malicious actors and the seriousness of the threat they pose.

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

There are many cases in the public domain involving disgruntled insiders. For example, Shakuntla Devi Singla used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1,800 hours to recover and reenter the lost data. Ms. Singla was convicted and sentenced to five months in prison, five months home detention, and ordered to pay $35,000 in restitution.

In January and February 1999 the National Library of Medicine (NLM) computer system, relied on by hundreds of thousands of doctors and medical professionals from around the world for the latest information on diseases, treatments, drugs, and dosage units, suffered a series of intrusions where system administrator passwords were obtained, hundreds of files were downloaded which included sensitive medical "alert" files and programming files that kept the system running properly. The intrusions were a significant threat to public safety and resulted in a monetary loss in excess of $25,000. FBI investigation identified the intruder as Montgomery Johns Gray, III, a former computer programmer for NLM, whose access to the computer system had been revoked. Gray was able to access the system through a "backdoor" he had created in the programming code. Due to the threat to public safety, a search warrant was executed for Gray's computers and Gray was arrested by the FBI within a few days of the intrusions. Subsequent examination of the seized computers disclosed evidence of the intrusion as well as images of child pornography. Gray was convicted by a jury in December 1999 on three counts for violation of 18 U.S.C. 1030. Subsequently, Gray pleaded guilty to receiving obscene images through the Internet, in violation of 47 U.S.C. 223.

Hackers.—Hackers 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. More 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 recent denial-of-service attacks are merely illustrations of the disruption that can be caused by tools now readily available on the Internet. Hacks can also be mistaken for something more serious. This happened initially in the Solar Sunrise case, discussed below.

Hactivism.—Recently we have seen a rise in what has been dubbed "hacktivism"—politically motivated attacks on publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into web sites to send a political message. While these attacks generally have not altered op-

erating systems or networks, they still damage services and deny the public access to websites containing valuable information and infringe on others' rights to communicate. One such group is called the "Electronic Disturbance Theater," which promotes civil disobedience on-line in support of its political agenda regarding the Zapatista movement in Mexico and other issues. This past spring they called for worldwide electronic civil disobedience and have taken what they term "protest actions" against White House and Department of Defense servers. In addition, during the recent conflict in Yugoslavia, hackers sympathetic to Serbia electronically "ping" attacked NATO web servers. Russians, as well as other individuals supporting the Serbs, attacked websites in NATO countries, including the United States, using virus-infected e-mail and hacking attempts.

Supporters of Kevin Mitnick hacked into the Senate webpage and defaced it in May and June of last year. Mitnick had pled guilty to five felony counts and was sentenced in August 1999 to 46 months in federal prison and ordered to pay restitution. Mitnick was released from custody in January 2000 after receiving credit for time served on prior convictions.

The Internet has enabled new forms of political gathering and information sharing for those who want to advance social causes; that is good for our democracy. But illegal activities that disrupt e-mail servers, deface web-sites, and prevent the public from accessing information on U.S. Government and private sector web sites should be regarded as criminal acts that deny others their First Amendment rights to communicate rather than as an acceptable form of protest.

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

The Melissa Macro Virus was a good example of our response 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. On the investigative side, the NIPC acted as a central point of contact for the field offices who worked leads on the case. A tip received by the New Jersey State Police from America Online, and their follow-up investigation with the FBI's Newark Field Office, led to the April 1, 1999 arrest of David L. Smith. Search warrants were executed in New Jersey by the New Jersey State Police and FBI Special Agents from the Newark Field Office. Mr. Smith pleaded guilty to one count of violating Title 18, U.S.C. 1030 in Federal Court. Smith stipulated to affecting one million computer systems and causing $80 million in damage.

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

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

Distributed Denial of Service Attacks.—In the fall of 1999, the NIPC began receiving reports about a new threat on the Internet—Distributed Denial of Service Attacks. In these cases, hackers plant tools such as Trinoo, Tribal Flood Net (TFN), TFN2K, or Stacheldraht (German for barbed wire) on a number of unwitting victim systems. Then when the hacker sends the command, the victim systems in turn begin sending messages against a target system. The target system is overwhelmed with the traffic and is unable to function. Users trying to access that system are

denied its services. The NIPC issued an alert regarding these tools in December 1999 in order to notify the private sector and government agencies about this threat. Moreover, the NIPC's Special Technologies and Applications Unit (STAU) created and released to the public a software tool that enables system administrators to identify DDOS software installed on victimized machines. The public has downloaded these tools tens of thousands of times from the web site, and has responded to the FBI by reporting many intrusions and installations of the DDOS software. The public received the NIPC tool so well that the computer security trade group SANS awarded their yearly Security Technology Leadership Award to members of the STAU. The availability of this tool has helped facilitate our investigations of ongoing criminal activity by uncovering evidence on victim computer systems.

On February 8, 2000, the FBI received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship the NIPC has developed with the private sector, in the days that followed, several other companies also reported denial of service outages. These companies cooperated with our National Infrastructure Protection and Computer Intrusion squads in the FBI field offices and provided 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.

The resources required in these investigations can be substantial. Already we have five FBI field offices with cases opened: Los Angeles, San Francisco, Atlanta, Boston, and Seattle. Each of these offices has victim companies in its jurisdiction. In addition, so far seven field offices are supporting the five offices that have opened investigations. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers, and providing all-source analytical assistance to field offices. Agents from these offices are following up literally hundreds of leads. While the crime may be high tech, investigating it involves a substantial amount of traditional police work as well as technical work. For example, in addition to following up leads, NIPC personnel need to review an overwhelming amount of log information received from the victims. Much of this analysis needs to be done manually. Analysts and agents conducting this analysis have been drawn off other case work. In the coming years we expect our case load to substantially increase.

Terrorists.—Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. For example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. Moreover, some groups have already used cyber attacks to inflict damage on their enemies' information systems. For example, a group calling itself the Internet Black Tigers conducted a successful "denial of service" attack on servers of Sri Lankan government embassies. Italian sympathizers of the Mexican Zapatista rebels attacked web pages of Mexican financial institutions. Thus, while we have yet to see a significant instance of "cyber terrorism" with widespread disruption of critical infrastructures, all of these facts portend the use of cyber attacks by terrorists to cause pain to targeted governments or civilian populations by disrupting critical systems.

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

Sensitive Intrusions.—In the last two years we have seen a series of intrusions into numerous Department of Defense computer networks as well as networks of other federal agencies, universities, and private sector entities. Intruders have successfully accessed U.S. Government networks and taken enormous amounts of unclassified but sensitive information. In investigating these cases, the NIPC has been coordinating with FBI Field Offices, Legats, the Department of Defense (DOD), and other government agencies, as circumstances require. The investigation has determined that these intrusions appear to originate in Russia. The NIPC has also supported other very sensitive investigations, including the possible theft of nuclear secrets from Los Alamos National Laboratory in New Mexico. It is important that the

Congress and the American public understand the very real threat that we are facing in the cyber realm, not just in the future, but now.

Information Warfare.—One of the greatest potential threats to our national security is the prospect of "information warfare" by foreign militaries against our critical infrastructures. We know that several foreign nations are already developing information warfare doctrine, programs, and capabilities for use against each other and the United States or other nations. Foreign nations are developing information warfare programs because they see that they cannot defeat the United States in a head-to-head military encounter and they believe that information operations are a way to strike at what they perceive as America's Achilles Heel—our reliance on information technology to control critical government and private sector systems. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. A serious challenge we face is even recognizing when a nation may be undertaking some form of information warfare. If another nation launched an information warfare attack against the United States, the NIPC would be responsible to gather information on the attack and work with the appropriate defense, intelligence, and national command authorities.

Traditional Threats to Society Moved to the Cyber Realm

Computers and networks are not just being used to commit new crimes such as computer intrusions, denial of service attacks, and virus propagation, but they are also facilitating some traditional criminal behavior such as extortion threats, fraud and the transmission of child pornography. For example, the NIPC recently supported an investigation involving e-mail threats sent to a Columbine High School student threatening violence.

Child Pornography and Exploitation.—While the Internet has been a tremendous boon for information sharing and for our economy, it unfortunately has also become a zone where predators prey on the weakest and most vulnerable members of our society, our children. The sex offender using a computer is not a new type of criminal. Rather it is simply a case of modern technology being combined with an age old problem. The use of computers has made child pornography more available now than at any time since the 1970s. An offender can use a computer to transfer, manipulate, or even create child pornography. Images can be stored, transferred from video tape or print media, and transmitted via the Internet. With newer technology, faster processors and modems, moving images can now also be transmitted. In addition, the information and images stored and transmitted can be encrypted to deter or avoid detection. As computers and technological enhancements, such as faster modems and processors, become less expensive and more sophisticated, the potential for abuse will grow.

CHALLENGES TO LAW ENFORCEMENT IN INVESTIGATING CYBERCRIME

The burgeoning problem of cybercrime poses unique challenges to law enforcement. These challenges require novel solutions, close teamwork among agencies and with the private sector, and adequate numbers of trained and experienced agents and analysts with sophisticated equipment.

Identification and Jurisdictional Challenges

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

The timing of the intrusions and links to some Internet Service Providers in the Gulf region caused many to believe that Iraq was behind the intrusions. The investigation, however, revealed that two juveniles in Cloverdale, California, and several individuals in Israel were the culprits. Solar Sunrise thus demonstrated to the

interagency community how difficult it is to identify an intruder until facts are gathered in an investigation, and why assumptions cannot be made until sufficient facts are available. It also vividly demonstrated the vulnerabilities that exist in our networks; if these individuals were able to assume "root access" to DOD systems, it is not difficult to imagine what hostile adversaries with greater skills and resources would be able to do. Finally, Solar Sunrise demonstrated the need for interagency coordination by the NIPC.

Jurisdictional Issues.—Another significant challenge we face is hacking in multiple jurisdictions. A typical hacking 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 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. 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. Our Legats are working very hard to build bridges with local law enforcement to enhance cooperation on cyber crime. The NIPC has held international computer crime conferences with foreign law enforcement officials to develop liaison contacts and bring these officials up to speed on cybercrime issues. We have also held cybercrime training classes for officers from partner nations.

Despite the difficulties, we have had some success in investigating and prosecuting these crimes. In 1996 and 1997, the National Oceanic and Atmospheric Administration (NOAA) suffered a series of computer intrusions that were linked to a set of intrusions occurring at the National Aeronautics and Space Administration (NASA). Working with the Canadian authorities, it was determined that the subject resided in Canada. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, he pled guilty to 12 counts of computer intrusions and the Canadian Superior Court of Justice sentenced him to 6 months in jail for each of the counts, with the sentences running concurrently. In another case, Peter Iliev Pentchev, a Princeton University student, was identified as an intruder on an e-commerce system. An estimated 1,800 credit card numbers, customer names, and user passwords were stolen. The company had to shut down its web servers for five days to repair the damages estimated at $100,000. Pentchev has fled to his native Bulgaria and the process is being determined to return Pentchev to the United States to face charges.

In 1994–95, an organized crime group headquartered in St. Petersburg, Russia, transferred $10.4 million from Citibank into accounts all over the world. After investigation by the FBI's New York field office, all but $400,000 of the funds were recovered. Cooperation with Russian authorities helped bring Vladimir Levin, the perpetrator, to justice. In another case, the FBI investigated Julio Cesar Ardita, an Argentine computer science student who gained unauthorized access to Navy and NASA computer systems. He committed these intrusions from Argentina, and Argentine authorities cooperated with the FBI on the investigation. While he could not be extradited for the offenses, he returned voluntarily to the United States and was sentenced to three years probation. In all of these cases, Legats have been essential to the investigation. As the Internet spreads to even more countries, we will see greater demand placed on the Legats to support computer intrusion investigations.

Human and Technical Challenges

The threats we face are compounded by human and technical challenges posed by these types of investigations. The first problem is, of course, having enough positions for agents, computer scientists, and analysts to work computer intrusions. Once we have the authorized positions, we face the issue of recruiting people to fill these positions, training them in the rapidly changing technology, and retaining them. There is a very tight market out there 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.

Our current resources are stretched paper thin. We only have 193 agents assigned to NIPC squads and teams nationwide. Major cases, such as the recent DDOS attacks on Yahoo, draw a tremendous amount of personnel resources. Most of our technical analysts will have to be pulled from other work to examine the log files received from the victim companies. Tracking down hundreds of leads will absorb the energy of a dozen field offices. And this is all reactive. My goal is for the FBI to become proactive in this area just as we have in other areas such as drugs and

violent crime. In a few minutes I'll discuss what we need to do to improve our cybercrime fighting capabilities to become proactive in fighting cybercrime.

The technical challenges of fighting crime in this arena are equally vast. We can start just by looking at the size of the Internet and its exponential growth. Today it is estimated that more than 60,000 individual networks with 40 million users are connected to the Internet. Thousands of more sites and people are coming on line every month. In addition, the power of personal computers is vastly increasing. The FBI's Computer Analysis Response Team (CART) examiners conducted 1,260 forensic examinations in 1998 and 1,900 in 1999. With the anticipated increase in high technology crime and the growth of private sector technologies, the FBI expects 50 percent of its caseload to require at least one computer forensic examination. By 2001, the FBI anticipates the number of required CART examinations to rise to 6,000.

It is important to note that personnel resources with very specific technical skills are required not only for computer and Internet based crimes such as the DDOS incidents, but are increasingly necessary for more traditional matters as well. Examples of this type of problem include the approximately 6,000 man hours that the NIPC was required to expend investigating a recent computer-based espionage case. The NIPC's Special Technologies and Applications Unit (STAU) received approximately one million raw files from CART, and was required by the investigators to reproduce the activities of individuals over a period of years from that raw data. The amount of information which was required to be processed by STAU, and is still necessary to process, would fill the Library of Congress nearly twice. This type of case illustrates where technical analysis of the highest order has become necessary in sophisticated espionage matters. A recent extortion and bombing illustrate how traditional violent criminals are also turning to high technology. In this extortion case, the bomber's demands included that the victim post their responses to his requirements on their web site. The STAU was required to sort through millions of web site "hits" to discern which entries may have come from the bomber. Based on information generated by the STAU's efforts, agents were able to trace the bomber to a specific telephone line to his home address.

Clearly, the FBI needs engineering personnel to develop and deploy sophisticated electronic surveillance capabilities in an increasingly complex and technical investigative environment, skilled CART personnel to conduct the computer forensics examinations to support an increasingly diverse set of cases involving computers, as well as expert NIPCI personnel to examine network log files to track the path an intruder took to his victim. In cases such as Los Alamos or Columbine, both NIPCI and CART personnel were called in to bring their unique areas of expertise to bear on the case.

During the last part of 1998, most computers on the market had hard drives of 6–8 gigabytes (GB). Very soon 13–27 GB hard drives will become the norm. By the end of 2000, we will be seeing 60–80 GB hard drives. All this increase in storage capacity means more data that must be searched by our forensics examiners, since even if these hard drives are not full, the CART examiner must review every bit of data and every area of the media to search for evidence.

The FBI has an urgent requirement for improved tools, techniques and services for gathering, processing, and analyzing data from computers and computer networks to acquire critical intelligence and evidence of criminal activity. Over the past three years, the FBI's Laboratory Division (LD) has been increasingly requested to provide data interception support for such investigative programs as: Infrastructure Protection, Violent Crimes (Exploitation of Children, Extortion), Counterterrorism, and Espionage. In fact, since 1997, the LD has seen a dramatic increase in field requests for assistance with interception of data communications. Unless the FBI increases its capability and capacity for gathering and processing computer data, investigators and prosecutors will be denied timely access to valuable evidence that will solve crimes and support the successful prosecutions of child pornographers, drug traffickers, corrupt officials, persons committing fraud, terrorists, and other criminals.

One of the largest challenges to FBI computer investigative capabilities lies in the increasingly widespread use of strong encryption. The widespread use of digitally-based telecommunications technologies, and the unprecedented expansion of computer networks incorporating privacy features/capabilities through the use of cryptography (i.e. encryption), has placed a tremendous burden on the FBI's electronic surveillance technologies. Today the most basic communications employ layers of protocols, formatting, compression and proprietary coding that were non-existent only a few years ago. New cryptographic systems provide robust security to conventional and cellular telephone conversations, facsimile transmissions, local and wide area networks, Internet communications, personal computers, wireless trans-

missions, electronically stored information, remote keyless entry systems, advanced messaging systems, and radio frequency communications systems. The FBI is already encountering the use of strong encryption. In 1999, 53 new cases involved the use of encryption.

The FBI is establishing a centralized capability for development of investigative tools which support the law enforcement community's technical needs for cybercrime investigations, including processing and decrypting lawfully intercepted digital communications and electronically stored information. A centralized approach is appropriate since state and local law enforcement have neither the processing power nor trained individuals to assume highly complex analysis or reverse engineering tasks. The fiscal year 2001 budget includes $7,000,000 for this effort.

The need for a law enforcement centralized civilian resource for processing and decrypting lawfully intercepted digital communications and electronically stored information is well documented in several studies, including:

—The National Research Council's Committee Report entitled "Cryptography's Role in Securing the Information Society." Specifically, the Committee recommended that high priority be given to the development of technical capabilities, such as signal analysis and decryption, to assist law enforcement in coping with technological challenges.

—In 1996, Public Law 104–132 Section 811, the 104th Congress acknowledged the critical need and authorized the Attorney General to "* * * support and enhance the technical support [capabilities] * * *" of the FBI.

—The Administration policy position as set forth in the September 16, 1998, press release acknowledges that "The Administration intends to support FBI's establishment of a technical support [capability] to help build the technical capacity of law enforcement—Federal, State, and local—to stay abreast of advancing communications technology."

It has been the position of the FBI that law enforcement should seek the voluntary cooperation of the computer hardware and software industry as a means of attempting to address the public safety issues associated with use of encryption in furtherance of serious criminal activity. Over the past year and a half, the FBI has initiated an aggressive industry outreach strategy to inform industry of law enforcement's needs in the area of encryption, to continue to encourage the development of recoverable encryption products that meet law enforcement's needs, and to seek industry's assistance regarding the development of law enforcement plaintext access "tools" and capabilities when non-recoverable encryption products are encountered during the course of lawful investigations.

The FBI will be meeting this year with industry in an environment wherein various computer and software industry representatives can exchange technical and business information regarding encryption and encryption products with law enforcement. This information will assist law enforcement agencies with establishing development and operational strategies to make the most effective use of limited resources.

State and Local Assistance

Just as with other crimes, often the state and local authorities are going to be the first ones on the scene. The challenge for these law enforcement officers is even greater than the one the Federal Government faces in that state and local law enforcement is less likely to have the expertise to investigate computer intrusions, gather and examine cyber media and evidence. The challenge for the federal government is to provide the training and backup resources to the state and local levels so that they can successfully conduct investigations and prosecutions in their jurisdictions. This sort of cooperation is already showing results. For example, the FBI worked with the New Jersey State Police on the Melissa Macro Virus case that resulted in the arrest of David L. Smith by the New Jersey authorities. In addition, the NIPC and our Training Division are working together to provide training to state and local law enforcement officers on cybercrime. In fiscal year 1999 over 383 FBI Agents, state and local law enforcement and other government representatives have taken NIPC sponsored or outside training on computer intrusion and network analysis, energy and telecommunications key assets. We have made great strides in developing our training program for state and local law enforcement officials. More NIPC training than ever before is being conducted outside of Washington, DC, meaning that more state and local officers should have the opportunity to attend these classes with less disruption to their schedules and less travel. One of the main responsibilities of the NIPC Training and Continuing Education Unit is to develop and manage the state and local Law Enforcement Training Program. This program trains state and local law enforcement officials in a myriad of state-of-the-art cyber courses.

Building on the success of the San Diego Regional Computer Forensic Laboratory, the Attorney General asked the FBI and the Office of Justice Programs, to work in partnership to develop a series of regional laboratories. These facilities will provide computer forensic services as joint ventures among federal, state and local law enforcement. Six million dollars is requested in the Office of Justice Programs to establish several regional computer forensic laboratories. Working together, we are identifying geographical areas where the establishment of such partnerships could make significant impact.

The NIPC is supporting the Attorney General's proposal to create a network of federal, state, and local law enforcement personnel for combating cybercrimes. We are instructing each field office to have a point of contact at the appropriate investigative agencies regarding their area of jurisdiction and to provide this information to NIPC at FBIHQ.

Presidential Decision Directive (PDD) 63 identified the Emergency Law Enforcement Services Sector (ELES) as one of the eight critical infrastructures. PDD 63 further designated the Federal Bureau of Investigation as the lead agency with protecting the ELES. The NIPC is currently working on a strategic plan for this sector and holding meetings with sector representatives. This involves developing and implementing a plan to help law enforcement protect its own systems from attack so it will be able to deliver vitally needed services to the public.

Success of the NIPC requires building on proven mechanisms to develop and maintain long-term relationships with state and local law enforcement agencies. NIPC oversees outreach programs, coordinates training, shares information and coordinates interagency efforts to plan for, deter, and respond to cyber attacks.

Currently, the NIPC is sharing information with state and local governments via Law Enforcement On-line (LEO) and the National Law Enforcement Telecommunications System. Timely coordination and sharing of information with other law enforcement agencies is essential in combating the cyber threat in the Information Age. Local law enforcement is also encouraged to join the InfraGard chapters in their area.

State and local agencies investigate and prosecute cyber crimes based on violations of local laws. By sharing investigative data with the NIPC, emerging trends can be identified, analyzed and further shared with other agencies to share investigative responsibilities with their local FBI field office and the NIPC. The cross-jurisdictional nature of cyber crimes, in which attacks occur outside the state or even national borders, means that investigative efforts must be coordinated among local, state and federal agencies to ensure effective prosecution.

FBI CYBERCRIME INVESTIGATION CAPABILITIES

National Infrastructure Protection Center

Under PDD–63, the NIPC's mission is to detect, warn of, respond to, and investigate computer intrusions and unlawful acts that threaten or target our critical infrastructures. The Center not only provides a reactive response to an attack that has already occurred, but proactively seeks to discover planned attacks and issues warnings before they occur. This large and difficult task requires the collection and analysis of information gathered from all available sources (including law enforcement investigations, intelligence sources, data voluntarily provided by industry and open sources) and dissemination of analyses and warnings of possible attacks to potential victims, whether in the government or the private sector. To accomplish this mission, the NIPC relies on the assistance of, and information gathered by the FBI's 56 field offices, other federal agencies, state and local law enforcement, and perhaps most importantly, the private sector.

The NIPC, while located at the FBI, is an interagency center, with representatives from many other agencies, including DOD, the U.S. Intelligence Community, and other federal agencies. The NIPC at FBI Headquarters currently has 79 FBI personnel, with an authorized ceiling of 94. There are 22 representatives from Other Government Agencies (OGAs), the private sector, state and local law enforcement, and our international partners at the Center. Our target for OGA and private sector participation is 40.

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 program manages computer intrusion investigations conducted by FBI field offices throughout the country: provides subject matter experts, equipment, and technical support to cyber investigators in federal, state and local government agencies involved in critical infrastructure protection; and provides a cyber emergency response capability to help resolve a cyber incident.

The Analysis and Warning Section (AWS) serves as the indications and warning arm of the NIPC. It provides analytical support during computer intrusion investigations and long-term analyses of vulnerability and threat trends. Through its 24/7 watch and warning capability, it distributes tactical warnings and analyses to all the relevant partners, informing them of potential vulnerabilities and threats and long-term trends. It also reviews numerous government and private sector databases, media, and other sources daily to gather information that may be relevant to any aspect of our mission, including the gathering of indications of a possible attack.

The Training, Outreach and Strategy Section (TOSS) coordinates the training and education of cyber investigators within the FBI field offices, state and local law enforcement agencies, and private sector organizations. It also coordinates outreach to private sector companies, state and local governments, other government agencies, and the FBI's field offices. In addition, this section manages collection and cataloguing of information concerning "key assets" across the country. Finally, it handles our strategic planning and administrative functions with FBI and DOJ, the National Security Counsel, other agencies and Congress.

Through these, the Center brings its unique perspective as the only national organization devoted to investigation, analysis, warning, and response to attacks on the infrastructures. Further, as an interagency entity, the NIPC takes a broad view of infrastructure protection, looking not just at reactive investigations but also at proactive warnings and prevention. Finally, through the FBI, the Center has a national reach to implement policy. The Center is working closely on policy initiatives with its Federal partners and meets regularly with the other Federal lead agencies on policy issues.

National Infrastructure Protection and Computer Intrusion Squads/Teams

In October 1998, the National Infrastructure Protection and Computer Intrusion Program (NIPCIP) was approved as an investigative program and resources were created and placed in each FBI field office with the NIPC at FBI Headquarters acting as program manager.

By the end of this fiscal year, there will be 16 FBI Field Offices with regional NIPC squads. Each of these squads will be staffed with 7 to 8 agents. Nationwide, there are 193 agents dedicated to investigating NIPC matters. In order to maximize investigative resources the FBI has taken the approach of creating regional squads that have sufficient size to work difficult major cases and to assist those field offices without an NIPC 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.

Computer Analysis and Response Teams (CART)

An essential element in the investigation of computer crime is the recovery of evidence from electronic media. In a murder investigation, the detectives investigate the case but the coroner examines the body for evidence of how the crime was committed. The CART personnel serve this function in cyber investigations. CART examiners perform three essential functions. First, they extract data from computer and network systems, and conduct forensic examinations and on-site field support to all FBI investigations and programs where computers and storage media are required as evidence. Second, they provide technical support and advice to field agents conducting such investigations. Finally, they assist in the development of technical capabilities needed to produce timely and accurate forensic information.

Currently the FBI has 26 full time CART personnel at FBI Headquarters and 62 full-time and 54 part-time CART personnel in the field, for a total of 142 trained CART personnel. CART resources are used in a variety of investigations ranging from sensitive espionage cases to health care fraud. For example, on September 12, 1998, the FBI executed the arrest of individuals who were involved in an espionage ring trying to penetrate U.S. military bases on behalf of the Cuban government. During the arrest of these individuals CART conducted the seizure of 35 Gb of digital evidence to include personal computers containing twelve (12) hard drives, 2,500 floppy diskettes, and assorted CD–ROMs. The FBI deployed more than 30 CART field examiners during the search and examination which consumed thousands of hours of their time.

In order to process the vast quantities of information required, the CART program needs to purchase or develop new ways of handling digital evidence. One program used by the FBI is the Automated Computer Examination System (ACES), a data exploration tool developed by the FBI Laboratory, to scan thousands of files for identification of known format and executable program files. ACES verifies that certain

program, batch or executable files are for computer operation and do not represent a file in which potential evidentiary material is stored. Results from an ACES examination can be passed to other analytical utilities used in examining a computer.

The FBI is also working with other federal agencies as well as state and local law enforcement to share data and forensic expertise. In San Diego, a regional computer forensic capability has been established that is staffed by the FBI, the Navy, and the San Diego police department, among others. This lab serves as a resource for the entire region. The vast majority of all computer related seizures in San Diego County are currently being made through the RCFL. During the start-up period (Summer 1999 to December 1999), although all participating agencies had been co-located, each examiner had been working on his own agencies's cases. As of January 3, 2000, the San Diego lab started receiving submissions as a joint facility and jointly tracking those submissions. As of February 3, the lab had received 26 cases, including three federal cases consisting of large scale networks, and local cases including a death threat to a Judge, a poisoning case, and a child molestation case. We recognize that state and local law enforcement often will not have the resources for complex computer forensics, and we hope that the San Diego model can be expanded.

Technical Investigative Support

The FBI has long had capabilities regarding the interception of conventional phone lines and modems. The rapid advance of data technologies and the unregulated nature of the Internet has resulted in a myriad of technologies and protocols which make the interception of data communications extremely difficult. It is critical that the FBI properly equip investigators with technical capabilities for utilizing the critical investigative tools on lawfully authorized Title III and Title 50 interception.

Innocent Images Initiative/Child Pornography

The FBI has moved aggressively against child pornographers. In 1995 the FBI's first undercover operation, code name Innocent Images, was initiated. Almost five years later, Innocent Images is an FBI National Initiative, supported by annual funding of $10 million, with undercover operations in eleven FBI field offices—Baltimore, Birmingham, Cleveland, Dallas, Houston, Las Vegas, Los Angeles, Newark, Phoenix, San Francisco, and Tampa—being worked by task forces that combine the resources of the FBI with other federal, state and local law enforcement officers from Maryland, Virginia, the District of Columbia, Alabama, Ohio, Texas, Nevada, California, New Jersey, Arizona, and Florida. Investigations developed by the National Initiative's undercover operations are being conducted by every field office and information has been referred to foreign law enforcement agencies through the FBI's Legal Attaché Offices.

During fiscal year 1999 a total of 1,497 new cases were opened. Every one of these investigations has digital evidence and requires the assistance of a CART examiner. Additionally, 188 search warrants and 57 consent searches were executed, and 193 arrests, 125 indictments, 29 information and 108 convictions were obtained as a result of the Innocent Images National Initiative. Also in fiscal year 1999, the IINI provided 227 presentations to 17,522 individuals from foreign and domestic law enforcement and government officials, civilian groups, and private citizens in an effort to raise awareness about child pornography/child sexual exploitation issues and increase coordination between federal, state and local law enforcement.

Intellectual Property Rights/Internet Fraud

Intellectual property is the driver of the 21st century American economy. In many ways it has become what America does best. The United States is the leader in the development of creative, technical intellectual property. Violations of Intellectual Property Rights, therefore, threaten the very basis of our economy. Of primary concern is the development and production of trade secret information. The American Society of Industrial Security estimated the potential losses at $2 billion per month in 1997. Pirated products threaten public safety in that many are manufactured to inferior or non-existent quality standards. A growing percentage of IPR violations now involve the Internet. There are thousands of web sites solely devoted to the distribution of pirated materials. The FBI has recognized, along with other federal agencies, that a coordinated effort must be made to attack this problem. The FBI, along with the Department of Justice, U.S. Customs Service, and other agencies with IPR responsibilities, will be opening an IPR Center this year to enhance our national ability to investigate and prosecute IPR crimes through the sharing of information among agencies.

One of the most critical challenges facing the FBI and law enforcement in general, is the use of the Internet for criminal purposes. Understanding and using the Inter-

net to combat Internet fraud is essential for law enforcement. The fraud being committed over the Internet is the same type of white collar fraud the FBI has traditionally investigated but poses additional concerns and challenges because of the new environment in which it is located. Internet fraud is defined as any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms, and E-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators. The accessability of such an immense audience coupled with the anonymity of the subject, require a different approach. The frauds range from simple geometric progression schemes to complex frauds. The Internet appears to be a perfect manner to locate victims and provides an environment where the victims don't see or speak to the fraud perpetrators. Anyone in the privacy of their own home can create a very persuasive vehicle for fraud over the Internet. In addition, the expenses associated with the operation of a "home page" and the use of electronic mail (E-mail) are minimal. Fraud perpetrators do not require the capital to send out mailers, hire people to respond to the mailers, finance and operate toll free numbers, etc. This technology has evolved exponentially over the past few years and will continue to evolve at a tremendous rate. By now it is common knowledge that the Internet is being used to host criminal behavior. The top ten most frequently reported frauds committed on the Internet include Web auctions, Internet services, general merchandise, computer equipment/software, pyramid schemes, business opportunities/franchises, work at home plans, credit card issuing, prizes/sweepstakes and book sales.

IMPROVING FBI CYBERCRIME CAPABILITIES

The last two years have seen tremendous strides in the development of the National Infrastructure Protection Center in both the Headquarters and field program. We have directed our resources into developing our prevention, detection, and response capabilities. This has meant recruiting talented personnel from both inside and outside the FBI, training those personnel, and developing investigative, analytic, and outreach programs. Most of these programs had to be developed from scratch, either because no program previously existed or because the program had to be reinvigorated from an earlier FBI incarnation.

The cyber crime scene is dynamic—it grows, contracts, and can change shape. Determining whether an intrusion is even occurring can often be difficult in the cyber world, and usually a determination cannot be made until after an investigation is initiated. The establishment of the NIPC has greatly enhanced the FBI's investigative, analytic, and case support capabilities. A few years ago, the NIPC would have been limited in its ability to undertake some of the sensitive investigations of computer intrusions that the FBI has supported. While the FBI has been able to develop and maintain its present response capability, the explosive nature of the crime problem continues to challenge our capacities. While much has been accomplished, much remains to be done.

Building Investigative Capacity

Trained personnel and resources present the greatest challenges to the FBI critical infrastructure protection mission. The FBI must make sure that the NIPC and Field Office squads are fully staffed with technologically competent investigators and analysts. It is also essential that these professional have state of the art equipment and connectivity they need to conduct their training.

To accomplish this, the FBI must identify, recruit, and train personnel who have the technical, analytical, investigative, and intelligence skills for engaging in cyber investigations. This includes personnel to provide early warnings of attacks, to read and analyze log files, write analytic reports and products for the field and the private sector, and to support other investigations with cyber components. With such a configuration of selected personnel skills, the FBI will be able to effectively and efficiently investigate cyber threats, allegations, incidents, and violations of the law that target and/or impact critical infrastructure facilities, components, and key assets. Aggressive recruitment of qualified specialists is critical. Targeting the right people and providing hiring and educational incentives are good steps in building this professional cadre.

Developing and deploying the best equipment in support of the mission is 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. NIPC must not only keep abreast of the criminal element but they must also accurately predict the next generation of criminal activity.

In order to support state and local law enforcement efforts, field offices will seek to form cybercrime task forces. This should include assigning a prosecutor to handle task force cases.

Building Partnerships with Industry and Academia

NIPC is founded on the notion of partnership. This partnership is critical to ensuring timely information sharing about threats and incidents, new technologies, and keeping our capabilities at the cutting edge. The FBI, in conjunction with the private sector, has also developed an initiative call "InfraGard" to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats. The initiative encourages the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each Field Office. Chapter membership includes representatives from the FBI, private industry, other government agencies, State and local law enforcement, and the academic community. The initiative provides four basic services to its members: an intrusion alert network using encrypted e-mail; a secure website for communication about suspicious activity or intrusions; local chapter activities; and a help desk for questions. The critical component of InfraGard is the ability of industry to provide information on intrusions to the local FBI Field Office using secure 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 law enforcement, intelligence, or industry information to determine if the intrusion is part of a broader attack on numerous sites. The Center can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. The secure website will also contain a variety of analytic and warning products that we can make available to the InfraGard community.

The NIPC has also developed and is implementing an aggressive outreach program. We have briefed a number of key critical infrastructure sector groups including the North American Electric Reliability Council and business groups such as the U.S. Chamber of Commerce. We are also working closely with our international partners.

Much attention has been given to the need to create mechanisms for sharing information with the private sector. The NIPC has built up a track record for doing this over the past 2 tears with concrete results. Not only has it provided early warnings and vulnerability threat assessments but it has also developed unique detection tools to help potential victims of DDOS attacks. And contrary to press statements by companies offering security services that private companies won't share information with law enforcement, private companies have reported incidents and threats to the NIPC or FBI. The cooperation we have received from victims in the recent DDOS attacks is only the most recent example of this. InfraGard will increase this capacity by providing a secure two way mechanism for sharing information between the government and the private sector.

Developing Forensic and Technical Capabilities

As noted above, CART has developed substantial capability to examine computer and network media and storage devices. But the rapid change in technology and the increasing use of computers in criminal activity necessitate the on-going development of better investigative and forensic tools and techniques for examiners. We fully expect that the number of cases requiring CART examinations will increase by over 50 percent in the next few years. In addition, as storage media hold more information, each individual examination will require more effort. To even attempt to keep pace with these developments, we will need to increase our personnel base in CART. For fiscal year 2001, funding is proposed to add 100 new CART examiners.

In addition, in order for our ACES program to remain able to provide comprehensive analysis of computer files, it needs to be continuously updated. After all, how many iterations of Windows®, Microsoft Office®, and other software and operating systems have we seen just in the last two years? We need to ensure that ACES can perform its function. The fiscal year 2001 budget includes $2,800,000 for the ACES program.

Improving our technical capabilities to access plaintext communications is a critical challenge to the FBI. The ultimate objective is to provide field investigators with an integrated suite of automated data collection systems, operating in a low-cost and readily available personal computer environment, which will be capable of identifying, intercepting and collecting targeted data of interest from a broad spec-

trum of data telecommunications transmissions mediums and networks. Substantial resource enhancements are required to progress development from current ad hoc, tactical data intercept systems to integrated modular systems, providing the field investigators with increased flexibility, simplicity and reliability and to enhance training programs to enable field Technically Trained Agents and Investigators to install and operate this complex equipment. The most technically complex component of electronic surveillance, has been and always will be the deciphering of encrypted signals and data. In the past few years, growth in electronic communications and the public demand for security have increased the number of investigations which encounter encrypted signals and data. With the convergence of digital technologies in the very near future, all electronic communications conducted using computers, the Internet, wireless and other forms of communications, will inherently incorporate and apply data security (i.e. encryption). The ability to gather evidence from FBI electronic surveillance and seized electronic data will significantly depend upon the development of and deployment of signal analysis and decryption capabilities. Funding enhancements are requested to step toward the fulfillment of a strategic plan to ensure that collected signals, data and evidence can be intercepted, interpreted and made usable in the prosecution of crimes and the detection of national security offenses. Failure to strategically prepare for the impending global changes data and voice telecommunications, information security, and the volumes of encrypted information collected by law enforcement pursuant to lawful court orders, will ensure that critical information and evidence will be unintelligible and unusable in future investigations.

We are urgently trying to develop our capabilities in this area through the acquisition of hardware and software tools, technologies and systems, and support services to work on a variety of research projects to meet this problem. Last September, the Administration announced a "New Approach to Encryption" which included significant changes to the nation's encryption export policies and recommended public safety enhancement to ensure "that law enforcement has the legal tools, personnel, and equipment necessary to investigate crime in an encrypted world."

Specifically, on September 16, 1999, the President, on behalf of law enforcement, transmitted to Congress the "Cyberspace Electronic Security Act of 1999" which would: ensure that law enforcement maintains its ability to access decryption information stored with third parties, while protecting such information from inappropriate release; protect sensitive investigative techniques and industry trade secrets from unnecessary disclosure in litigation or criminal trials involving encryption, consistent with fully protecting defendants' rights to a fair trial; and authorize $80 million over four years for the FBI's Technical Support Center (TSC), which serves as a centralized technical resource for federal, state and local law enforcement in responding to the increased use of encryption in criminal cases. The TSC is an expansion of the FBI's Engineering Research capabilities that will take advantage of existing institutional and technical expertise in this area. As indicated earlier, the fiscal year 2001 budget proposes an increase of $7,000,000 for the FBI's counterencryption program. We urge Congress to support us in these endeavors.

The law enforcement community relies on lawfully-authorized electronic surveillance as an essential tool for the investigation, disruption, and prevention of serious and violent offenses. Technological advances have taken a serious toll on law enforcement's ability to protect the public through the use of lawfully-authorized electronic surveillance. The Communications Assistance for Law Enforcement Act (CALEA) was passed so that the telecommunications industry would pro-actively address law enforcement's need and authority to conduct lawfully-authorized electronic surveillance as a basic element in providing service. CALEA clarifies and further defines existing statutory obligations of the telecommunications industry to assist law enforcement in executing lawfully-authorized electronic surveillance.

The FBI developed a flexible deployment strategy to minimize the costs and the operational impact of installation of CALEA-compliant software on telecommunications carriers. This strategy supports the carriers' deployment of CALEA-compliant solutions in accordance with their normal business cycles when this deployment will not delay implementation of CALEA solutions in high-priority areas. The carriers will provide projected CALEA-deployment schedules for all switches in their network and information pertaining to recent lawfully authorized electronic surveillance activity. Using this information, the FBI and the carrier will develop a mutually agreeable deployment schedule. The FBI provided the carriers with the Flexible Deployment Assistance Guide to facilitate the carrier's submission of information.

The FBI is negotiating with telecommunications carriers and manufacturers of telecommunications equipment for nationwide Right-to-Use (RTU) licenses to facilitate the availability of CALEA-compliant software to carriers. Also, the FBI is establishing a regional, nationwide law enforcement liaison program. This team will fa-

cilitate developing consensus law enforcement electronic surveillance requirements for all telecommunications technologies and services required to comply with CALEA; educate and inform Congress and the Federal Communications Commission (FCC) to ensure law enforcement's ability to conduct court-authorized electronic surveillance is not compromised on any telecommunications technology or service required to comply with CALEA; identify, publish, and ensure deployment of capacity requirements in accordance with Section 104 of CALEA; and develop a prioritized plan for the effective deployment and tracking of CALEA solutions.

The FBI needs to conduct testing and verification of manufacturer-proposed CALEA technical solutions and to have the subject matter expertise necessary to address new technologies that must comply with CALEA. Without these capabilities, the FBI will be unable to conduct testing and verification of manufacturer-proposed CALEA technical solutions and complete the nationwide RTU license agreements. The fiscal year 2001 budget proposes a total of $240,000,000 for CALEA RTU license agreements, including $120,000,000 under the Telecommunications Carrier Compliance Fund and $120,000,000 under the Department of Defense. Additionally, $2,100,000 is requested to support the FBI's CALEA program management office.

CONCLUSION

Computer crime is one of the most dynamic problems the FBI faces today. Just think about how many computers you have owned and how many different software packages you have learned over the past several years and you can only begin to appreciate the scope of the problem we are dealing with in the fast changing area. We need to budget for and train on technology that often has not even been invented when we begin the budget cycle some 18 months prior to the beginning of the fiscal year. I am proud of the progress that we have made in dealing with this problem. What I have tried to do here today is give you a flavor of what we are facing. I am confident that once the scope of the problem is clear, we can work together to develop the capabilities to meet the computer crime problem, in all its facets, head on. Our economy and public safety depend on it.

Senator GREGG. Thank you, Director. That was a very comprehensive summary of what you are doing and actually it sounded to me like a pretty good outline of a 5-year plan, which the Attorney General had mentioned earlier, or at least a base off of which to begin a 5-year plan.

STATEMENT OF HON. WILLIAM A. REINSCH, UNDER SECRETARY OF COMMERCE, EXPORT ADMINISTRATION, DEPARTMENT OF COMMERCE

Senator GREGG. Secretary Reinsch, I did not know if you wanted to throw in some comments here. We have a bit of a time issue, but please.

Mr. REINSCH. I have only three, Mr. Chairman, and I appreciate the courtesy. Let me say first that Secretary Daley very much appreciated your invitation to appear. He regrets he cannot be here. He is leading a business delegation to Latin America. He flew back from Brazil Monday night for the White House meeting on this subject yesterday morning and then he flew back to Argentina last night to rejoin the delegation. If nothing else, he is racking up frequent flier miles, and he apologizes for not being able to be with you. I think his presence yesterday indicates how important he felt this issue is.

Second, I did submit a statement for the record. I will not attempt to deliver it. I would like to excerpt from one paragraph of it, if I may, Mr. Chairman.

Senator GREGG. Please.

Mr. REINSCH. And that is the following, and it responds to, alludes to a point that you made. I want to make clear that while the Federal Government's responsibility in the critical infrastructure area is clear with respect to the commission of crimes, that is

only part of the equation. With respect to prevention and the development of more comprehensive security measures, the government can best play a supporting role. The infrastructure at risk is owned and operated by the private sector. Inevitably, it will be they who must work together to take the steps necessary to protect themselves.

The government can help. We can identify problems and publicize them. We can encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst, and that is precisely the role that the Commerce Department is playing in several ways. One, through the Critical Infrastructure Assurance Office's coordination of the development of a national plan, which the President released the first version of last month. Most recently through the convening of the Partnership for Critical Infrastructure Security, which I can comment on later if you are interested, which kicked off in New York in December, the next meeting of which will be next week. We already have some 180 people signed up to attend, so we are optimistic it is going to be a significant event in terms of developing a better means for companies to talk with each other about these problems.

Third, and finally, Mr. Chairman, I would be derelict in my duty and would be chastised by my superiors if I did not make a pitch for the money since I am in the appropriate forum to do that. I am sure it will be no surprise to you that we believe that we need and deserve every penny we have asked for, and we will be happy to provide support for that at the appropriate time. I am sure the Secretary will want to say something about that when he appears before you I believe either later this month or early next month.

I would just note in passing that the President's total budget in the critical infrastructure area projects a 15 percent increase across all the different functions including those that the Attorney General and the Director talked about. This is, in our judgment, an area where there is no one-size-fits-all solution. And that is reflected in the plan. It is reflected in the different activities by different agencies. It is also reflected in the budget request. Most of the money goes to the national security and law enforcement agencies, as it should.

A number of the other activities respond to some of the points you made, Mr. Chairman, and some of the things that you will be reading about in the papers in the future are handled elsewhere. For example, the Federal Cyber Services Training and Education Initiative which deals with precisely the problem you raised of the Federal Government's difficulty in obtaining and retaining skilled people is a program that is going to be handled through OPM and the National Science Foundation.

Other things like FIDNET, the Expert Review Teams, Public Key Infrastructure pilot programs; and R&D are handled partly through a variety of civilian entities or agencies, the most notable of which in terms of new requests is the request for NIST's Institute for Information Infrastructure Protection, or I^3P, which will finance longer-term research on the part of private sector universities and private sector actors for solutions to these problems. The President's budget includes not only 2001 request but a $9 million supplemental request for fiscal year 2000 to try to jumpstart some

of the programs I just alluded to. And with that, Mr. Chairman, I appreciate your time, and I would be happy to join in the questioning if you wish.

[The statement follows:]

PREPARED STATEMENT OF WILLIAM A. REINSCH

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

Inter-dependent 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. 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 while the Federal government's responsibility in this area is clear with respect to the commission of crimes, that is only part of the equation. With respect to prevention and the development of more comprehensive security measures, the government can best play a supporting role. The infrastructure at risk is owned and operated by the private sector. Inevitably, it will be they who must work together to take the steps necessary to protect themselves. We can help. We can identify problems and publicize them, encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst. That is precisely the role the Commerce Department is playing in several ways.

The Commerce Department, through its Critical Infrastructure Assurance Office (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.

Another active area is the creation 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 other stakeholders, including the risk management and investment communities, mainstream businesses, and state and local governments. It complements the NIPC's focus on cyber-terrorism by encouraging industry to collaborate on information security issues. Secretary Daley and I met with senior members of Partnership companies in December in New York. We will meet again next week in Washington, D.C., with senior members of the Partnership companies in order to encourage business leaders to adopt information security as an important business practice.

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.

President Clinton has increased funding for critical infrastructure substantially over the past three 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.

The Clinton Administration has developed and provided full or pilot funding for the following key initiatives designed to protect our computer systems:

—Establishing a permanent Expert Review Team (ERT) at NIST that will help agencies conduct vulnerability analyses and develop critical infrastructure protection plans. ($5 million).

—Funding seven Public Key Infrastructure model pilot programs in fiscal year 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 "patches" for known software defects. ($10 million).

—Developing Federal R&D Efforts. R&D investments in computer security will grow by 31 percent in the fiscal year 2001 budget. ($606 million).

—Establishing an Institute for Information Infrastructure Protection. Building on a Science Advisory Panel recommendation, the Institute is designed to fill gaps in both government and private sector cyber-security R&D. ($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 information technology industry, key sectors of the corporate economy, and academia.

In addition, the President announced a number of new initiatives designed to support efforts for enhancing computer security, including a $9 million fiscal year 2000 budget supplemental to jump-start key elements of next year's budget. Among these was funding for NIST to create the Institute for Information Infrastructure Protection (I^3P).

Yesterday 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 the past week 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 a secure business environment in order to ensure both our national security and the growth of our economy.

ADDITIONAL STATUTORY AUTHORITY REQUIREMENTS

Senator GREGG. Thank you. Yes, absolutely. Let us begin with some simple issues so we can sort of lay the groundwork here. Madam Attorney General or Director Freeh, do you believe there is any additional statutory authority in order to pursue the crimes that we are seeing?

Ms. RENO. We are going to consider additional tools to locate and identify the criminals. For example, we may need to strengthen the Computer Fraud and Abuse Act by closing the loophole that allows computer hackers who have caused a large amount of damage to a network of computers to escape punishment if no individual computer sustained over $5,000 worth of damage. I think that is important.

We may also need to update our trap and trace laws under which we are able to identify the origin and destination of telephone calls and computer messages. Under current law, in some instances, we must obtain court orders in multiple jurisdictions to trace a single communication. It might be extremely helpful, for instance, to provide a nationwide effect for trap and trace orders. We must also ensure that, in upgrading our computer crime fighting laws, appropriate privacy safeguards are maintained and wherever possible strengthened. For example, recent investigations have revealed serious violations of privacy by hackers who have obtained individ-

uals' personnel data such as credit cards and passwords. An increase in the penalty for violations of invasions into private stored communications may be appropriate. We would like to develop a thoughtful and effective package in working with your staff.

Senator GREGG. Director Freeh, do you have any further thoughts on that?

Mr. FREEH. The only thing I would add to that, and I think it is an issue that we are exploring, is whether some of this activity which is beyond a single episode of fraud or hacking, you know, gets into the realm of enterprise criminal activity. In other words, whether somebody or a group of people doing this is engaging in a criminal enterprise which, of course, would bring it under the racketeering statutes with much more substantial penalties than all these current predicate statutes. I do not think most of the statutes that are ordinarily employed are actually RICO predicates. I think it is an area that needs a lot of research and thought, but if you are talking about an international group of people that is engaging in activity with billions of dollars of potential loss and affecting millions of people, I am not so sure that should not be in the realm of much more serious coverage.

Senator GREGG. So you are saying we should apply RICO, potentially apply the RICO portion of the mechanism to these types of events?

Mr. FREEH. I think we should consider that and look at all the other forfeiture provisions that would obtain under that statute both criminally and civilly for people who are found to be doing this.

Senator GREGG. Can we expect to get a package then of suggestions in this area?

Ms. RENO. We are working to put together a package and I think you can anticipate that.

PRIVATE SECTOR VERSUS FEDERAL GOVERNMENT ROLE

Senator GREGG. That would be very helpful. The second threshold issue is this question of balancing the privacy versus the role of the government in the commercial activity. I know you have both alluded to this, and Secretary Reinsch made a very specific statement on this. Where do we cross the line? How far should the Government go, and what are the risks of interfering with the energy and the freedom of the Internet by having Government involvement in trying to discipline—discipline is the wrong term—in trying to pursue criminals who hack these sites?

Ms. RENO. I think that with respect to prevention, much can be done by the private sector with, as I suggested, the law enforcement agencies providing suggestions, thoughts and discussion as to what our experience in terms of the investigation of actual crime in this area has produced. That would indicate what steps could have been taken to have prevented it. But I do not think we should interrupt the energy of the Internet by doing it top down and suggesting that mandates and directives be imposed on the private sector. I think we can do so much if we build a partnership that is based on mutual respect and on our experience.

With respect to law enforcement investigations, I think we have got to be as measured with law enforcement investigations in the

area of cybercrime as we are with respect to any other crime. We must use the Attorney General's guidelines in a thoughtful, effective manner to ensure wherever we can appropriate privacy and that steps be taken to ensure enforcement of all Department procedures directed at ensuring privacy.

Senator GREGG. Anybody else want to comment on that general philosophical issue?

Mr. REINSCH. If I may, Mr. Chairman, I think the clearest point, of course, is when there is an attack or an imminent credible threat of an attack, when something is a crime or is about to be a crime. I think what you find is it certainly is appropriate for law enforcement to be directly and intimately involved at that point, and I think you find most private parties being very interested in their involvement at that point because of the clarity of the situation. Your question becomes more difficult when you are talking about days, weeks, months in advance of that situation.

And that creates a much more complicated situation. I think the Attorney General's comment is right on target and in particular the phrase she used, "building partnerships", is probably the best way to do this. That is mutual confidence. There is, in fact, a spectrum of opinion in the private sector on this as you would expect on everything. Some people, sometimes people who have an economic stake in these situations are a little less interested in privacy because they are interested in the economics. There are other people at the other end of the spectrum who will not cooperate with anybody in the Federal Government under any circumstances even if a crime were being committed because that is their philosophy and that is a problem that, you know, we have to deal with.

I think trying to narrow the extremes of that spectrum and build a critical mass of cooperation in the middle, which is what we ought to be striving for, really depends on exactly what the Attorney General said: creating structures that build mutual confidence, creating structures in which we—I think the civilian side of the government, if you will, law enforcement if you will—and the private sector all participate and can share information in an atmosphere of mutual confidence. We have to do that in a variety of different ways. I do not think there is one institution or one mechanism that is going to meet the needs of everybody in that situation, but I think that she is exactly right. That is the way to go about it.

COORDINATION AMONG FEDERAL AGENCIES

Senator GREGG. On the issue of coordination, it seems to me that we are dealing with a couple, a variety of different levels here, and let me see if I am adequately summarizing it, and please tell me if I am not. I want to get your comments on it. We have the terrorist event, and we have a variety of different agencies that are addressing the terrorist event. We have the commercial event and then we have the issue of putting forward a cooperative effort with the private sector in order to give the private sector tools that we may have developed within the government or which our expertise within the government is able to develop or which we are paying for to be developed and making those generally available to the public.

These different levels of activity seem to be functioning in various agencies without necessarily the coordination that we might want to see so that there is an overlap. My question is, is that a correct summary of what the different efforts are; and is there, in your sense, adequate coordination between Commerce, Justice, within Justice, between FBI and Justice, CIA, DARPA, NIST within Commerce, and the National Security Council which has decided to put its rather large foot into this issue?

First, are we working together on the terrorism issue? Second, are we working together on the commercial side? And third, are we working together on the issue of getting out information capacity to the private sector in a partnership way?

Mr. FREEH. Starting with the terrorism issue, I think the results are very, very good. Again, these coordinating efforts are probably only about 5 years old, which in the life of Government agencies is not a great deal of time. But over the last 5 years, the ability to coordinate investigations of active terrorism as well as responding to them I think has been steadily improving to the point where I believe it is very sufficient. Again, our getting back——

Senator GREGG. And is the FBI the lead agency on that within the Government?

Mr. FREEH. Yes, the FBI is the lead agency with respect to counterterrorism, law enforcement, prevention, protection both within the United States or overseas on behalf of the Federal Government.

[The information follows:]

FBI LEAD AGENCY ROLES

Under Presidential Decision Directive (PDD) 39, the Department of Justice, through the FBI, is designated lead responsibility for the operational response to terrorist incidents that take place within U.S. territory. PDD–39 also confers upon the Department of State, through U.S. Ambassadors, lead responsibility for serving as the on-scene coordinator for the response of the U.S. Government to international terrorist incidents that take place outside of U.S. territory, except when the exercise of military force is directed. In those instances, the Department of Defense is the lead agency until such time as the use of military force is terminated. The Federal Aviation Administration has lead responsibility for coordinating any law enforcement activity affecting the safety of persons aboard an aircraft during acts of air piracy. The order also reaffirms the FBI lead responsibility for investigating terrorist acts that are planned or carried out by either foreign or domestic terrorists in the United States or which are carried out by terrorists against United States citizens or institutions outside the territorial United States.

COORDINATION OF LAW ENFORCEMENT

Mr. FREEH. The events over the millennium period I think were the template of how that is supposed to work. The FBI operations center, which you supported, was up and running 24 hours a day for several weeks. We had representatives of every single Federal agency there, including all the security agencies. We were on-line in real-time with our foreign and State and local partners. Leads were covered. An investigation was conducted in extremely fast-moving circumstances 24 hours a day and it worked. It worked to the sense that there were no major breakdowns. There were some things we learned that we could improve and will improve upon. But the coordination, the advice and updates to both the NSC and the congressional committees was ongoing and effective.

We do not think we lost anything between the cracks during that very critical period with a case of momentous significance. We are not doing as well in the cybercrime and cyber-terror area only because this is a new challenge and the structures that are responsible for that coordination are new. The NIPC, which we mentioned, has multi-agency representation, private sector representation, but we are really just beginning this process. There are a lot of things, both on the NSC level as well as the interagency level, that need to be improved upon—new coordinating groups, structures, resources. But the good news is we are well on our way to doing that, and if we use the counterterrorism case as a model, we have been extremely successful in that area.

Senator GREGG. What are we doing? I mean is there a task force, an interagency task force that is presently functioning that is trying to work up the turf issues on this?

NATIONAL INFORMATION PROTECTION CENTER [NIPC]

Mr. FREEH. On the operational level, yes. There is the NIPC. Those are the people who are coordinating and doing the investigations, representing all the various agencies. On the policy level, as you said, you have new initiatives and new players and that is an area that needs to be improved.

ROLE OF THE NATIONAL SECURITY COUNCIL

Senator GREGG. What is the NSC's role as far as you are concerned relative to this exercise, and how constructive is it?

Ms. RENO. I would describe it this way. Law enforcement is pursuing its law enforcement coordination responsibilities through the NIPC. I think Secretary Reinsch would point out that there are separate issues that go to coordination with respect to industry in terms of what can be done to prevent the problem in the first place. As bankers groups have banking associations that address bank security issues, so that is being done and the Commerce Department, I think, is involved in that effort. The NSC is looking at it through its coordinating function and the President announced the first version of the National Plan for Information Systems Protection last month. It is an invitation to dialogue with industry, with Congress and others. It was drafted by an interagency group and attorneys from the Justice Department and the FBI participated. It contains a number of proposals for protecting critical infrastructures that are contained in the 2001 budget request, for instance, a cyberservices training and education initiative.

Secretary Reinsch can talk a little bit more about the non-law enforcement side, but for something that is so new, something that is developing, I think the coordination is good. It can always improve.

Mr. REINSCH. If I may, Mr. Chairman, I think the Attorney General's comments were exactly on target, particularly the last one, which is the same one that Director Freeh made, which I would also echo. This is essentially a start-up, and start-ups are always a little rough around the edges, and you should expect this one to be a little rough around the edges. It is no different from any other start-up.

These things are gradually being sorted out. It takes time. Sometimes it takes episodes like this to get the line straight. Where the lines are straightest is probably in the event category of the three categories you described: the terrorist event or the cyber hacker event. Those are areas where law enforcement really has the lead, and I do not have anything to say about how that operates.

The area that is more complicated is what you might categorize as the pre-event situation, which was your third scenario. What are we doing to build confidence? What are we doing to create structures that will operate and exist outside of specific attacks and try to create tools or best practices, if you will, that will make it harder for those attacks to occur in the first place? There you have the best example of what I said earlier about no one-size-fits-all solution.

There are a number of different parties who participate in that exercise and certainly law enforcement does participate and should participate and we encourage—we, the Commerce Department, encourage private parties to deal with law enforcement in exactly the way that Director Freeh has described. Our experience suggests, however, that not all of them are prepared to do that in exactly the way that he would like. And that is why we have focused on the development of some other devices or some other means of sharing information but focusing more on sharing information amongst the private parties themselves, trying to get people in the private sector to take leadership and take ownership of these issues, to speak for their sector.

I think the banking and financial sector probably for obvious reasons has been the lead in doing this and has set up a very effective ISAC, Information Sharing and Analysis Center. The different departments, Energy, Transportation, Commerce, et cetera, have plans in various stages of development to encourage the same thing for their sectors. What this does is put the people inside the U.S. Government that have functional expertise, if you will, in touch with the people that they already know anyway because they regulate them in other fora, or they work with them on a regular basis with respect to other programmatic activities.

In the case of the Commerce Department, we are doing this for information and telecommunications, and NTIA is doing that. We think this is a process that is going to take off. We see signs that the private sector, again, to a different extent in different sectors, is understanding the need for joint activities and cooperation amongst themselves, not necessarily involving us.

Events like that of 2 weeks ago frankly are wake-up calls to these companies to get busy, and that is happening, and I think what you will see over time is the development of private structures that will end up doing several things: promoting best practices, tools and information amongst themselves, and disseminating those things amongst themselves, and in the process building confidence in their relationship with the government so that people that are now nervous about interface directly with law enforcement will not be nervous in the future. That is the point that we are trying to get to, but I would not say that we are entirely there yet and I think, you know, the getting there is going to be a little bit two steps forward, one step backward from time to time.

CRITICAL INFRASTRUCTURE ASSURANCE OFFICE

Senator GREGG. That is good explanation by all of you on this point, but let me follow up with some specifics. The Commerce Department, as I understand it, has got a Critical Infrastructure Assurance Office; it has this Institute for Information Infrastructure Protection, which is the NIST office, the I³P you are calling it.

Mr. REINSCH. That is proposed.

Senator GREGG. And the new proposal from the President which is COMNIC. What was that?

Mr. REINSCH. That has not been proposed. And I believe that it will not be proposed. You have been reading the Wall Street Journal, and they were wrong, Mr. Chairman.

Senator GREGG. That will come as a shock to them, but OK.

Mr. REINSCH. It came as a shock to me because I talked to that reporter and did not talk about that, but that is not a proposal.

Senator GREGG. Well, I guess my question is, what do you have up and running at the Commerce Department right now which deals with this issue and what is their portfolio?

Mr. REINSCH. Several things. First of all, as you noted, the Critical Infrastructure Assurance Office, the CIAO, if you will, is the staff coordinating agency for many of these activities. It is administratively in the Commerce Department. It staffs us. It does a lot of the work with us. One of its people is sitting right behind me ready to catch me when I fall. It also supports the National Security Council's work in this area as well. And I did not—if I can digress just a second—I did not respond and should have to your previous question about the role of the NSC, which I know is something that has concerned you. On that I would just say that the NSC with the CIAO's help has really played the role of, first of all, of staffing the President on the issue, which is not an insignificant issue because the President is very interested in this. Second, an idea generator. Not all of them have flown, but some of them have. The Cyber Services idea came from the NSC.

These things do not just happen because somebody in the NSC thinks they are a good idea. They get circulated out to agencies. People comment. They get massaged, but the NSC has been a good idea generator and has been a good coordinator of a lot of the activity in the pre-event phase that I described. So that is the NSC.

To go back to Commerce, there is the CIAO. NIST has a long-standing relationship with NSA that goes back a number of years in the cybersecurity area in terms of developing standards which is what NIST's primary activity is in this area, algorithms, encryption standards, for example. That is a long-standing exercise of theirs.

INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION

They have had a modest increment of R&D funding this year for these related functions, and I have to defer to Ray Kammer to tell you exactly what is going on there. The significant research increment is, as you mentioned, or would be if you approved it, the I³P, the Institute for Information Infrastructure Protection, which although located at NIST is essentially going to be a virtual institution in the sense that NIST is not going to do the research. NIST

is going to use the money, in this case the request is $50 million, for grants to private parties including universities for research into longer-term solutions of this problem.

Senator GREGG. If we can stop there, how do you expect that to interface with already existing research projects such as the Carnegie Mellon CERT team; the Thayer School which was referred to; and the Oklahoma school which is specifically doing research right now on technologies and ways to respond to counterterrorism?

Mr. REINSCH. Well, I think the answer is different depending on the institution. With respect to CERT and organizations like CERT, I do not see an overlap because CERT is really focusing more on short-term, you know, intervention and response, developing tools to deal with situations as they come up. CERT has an active, ongoing relationship with a lot of people in the private sector to do that, and it has been very effective. CERT is not the only CERT. There are other ones as well.

What we are talking about here is sort of looking at this issue, developing longer-term tools. Now, in that case, I think certainly there are other activities going on already including at some of the institutions you alluded to. In this case, this would be a supplement. I think there is room for more activity.

Senator GREGG. Is it going to be coordinated though?

Mr. REINSCH. To the extent that there is Federal involvement, yes. Under PDD–63, the President's Science Adviser, the head of the Office of Science Technology Policy, is charged with coordinating Federal R&D, and he would be in charge of coordinating this piece of that as well. Now if a university is not interested in Federal funding and wants to do something on its own, that would be a different matter.

Senator GREGG. My concern is that this new institute, I^3P, appears to be coming forward with a portfolio that is already being served in part by institutes that were created by other functions of government, such as the Attorney General's office, the FBI or in some instances, State and CIA. We will just have to wait and see how it is drafted, but we will want to get into that in more depth. I recognize it is a new initiative.

Mr. REINSCH. If I may, one more thing, Mr. Chairman. This grew directly out of a recommendation from PCAST, the President's Committee of Advisors on Science and Technology. It was a private sector group of scientists that recommended to the President that he do this. Their actual recommendation proposed something larger than what we have proposed. Their belief was that while there is private activity in this area right now, there are gaps in it, and it is appropriate for the Federal Government to try to, first of all, inventory what is going on and then to try to come up with a modest amount of money to fill the gaps.

Senator GREGG. I do not doubt that that is absolutely true. I think my concern is, if we already have law enforcement aggressively financing some of this, we ought to make sure that there is coordination between research which is already being done and paid for by the Federal Government for law enforcement purposes that overlaps distinctly research which would come out of this NIST initiative. I am sure it will be a good initiative because NIST is a superb organization, in my opinion.

LAW ENFORCEMENT OUTREACH TO E-COMMERCE INDUSTRY

Madam Attorney General, where do we stand in your opinion in the effort to do outreach to the e-commerce industry? Do you feel comfortable that they are comfortable with you and with the FBI or do we need more work? We have another panel after you to second-guess you on this one.

Ms. RENO. I think they are getting comfortable and I think that many of them are. It is exciting to hear representatives of industry, of banks and others talk about how they have had an opportunity to work with the FBI at the local level, how impressed they are with the knowledge a particular agent may have, how impressed they are with the professionalism with which they pursue the investigation. And it is that type of relationship that does so much to build an understanding throughout the agency. So in some measures it will take time, but at the meeting yesterday I was gratified by comments made to me on the part of industry about what we were doing and the success we were having in building a partnership.

Our Computer Crime Section, for example, has established the Industry Information Group, which includes representatives from the major ISPs, telecommunications companies and other industry groups. The IIG meets regularly to discuss cybercrime and security issues. We have also forged a cooperative relationship with the Internet Alliance, a group that represents the largest ISPs. Last week, DOJ officials met with Internet Alliance to discuss cooperative efforts.

With respect to privacy, I continually try to emphasize that we do not want a surveillance society or a top down approach to cybersecurity. We want to build a partnership that permits an appropriate exchange of information based on our experience.

We have really, I think, done something else, too, that is exciting in terms of forming a partnership, the beginnings of partnership that I think is where we are going in the future. This idea came about once when I was speaking to an industry group. One of the representatives said my 13-year-old daughter knows that she should not open other people's mail, that she should not go in and rummage around in her sister's bedroom, and that she should respect the privacy of others, but she has not been taught about what she should and should not do on the Internet. Last April, I announced that the Department along with Harris Miller and Information Technology Association of America had formed the Cybercitizen Partnership, a national campaign to educate and raise awareness of computer responsibility. I expect that that campaign will be in full force in the near future.

These are some of the things that we are doing, Mr. Chairman. Yesterday I asked the industry representatives there if they would meet with me just on the law enforcement issue of what law enforcement can do to improve the partnership and to build the working relationship that is so vital. Nobody likes to get into a situation where they have to deal with law enforcement because that means that they have been a victim of a crime. That is not a pleasant experience in any circumstance, but the FBI is doing so much in

terms of outreach, in terms of working with others, to build that trust and that confidence. I think we have come a long way.

FBI RELATIONSHIPS WITH PRIVATE SECTOR

Senator GREGG. Director Freeh, did you have any comment on that?

Mr. FREEH. Just to supplement it a little bit, I agree with the Attorney General 100 percent. This relationship is going to take some time. I think if you look back at the early relationship between the FBI, for instance, and the banking industry, 40, 50 years ago, you see where that relationship has grown in terms of trust, reliability, support. We are building that with not just the new high tech industry but many of these other interrelated companies. We mentioned before the InfraGard program which the NIPC administers and that is resident in many of our divisions, will hopefully be resident in all 56 divisions. Those agents go out to the private sector in that particular division—banks, transportation, and energy—and say we need to sit down with you, you need to tell us about the things that have to be protected and how your systems and networks can be compromised. That requires somewhat of an act of faith by some of the companies to give that information and assistance, and then when an attack occurs have the confidence to report that.

It is much akin to working the economic espionage cases. Somebody has tried to steal a valuable trade secret of a company. The FBI comes in to do the investigation and asks basically to get all the information about that trade secret. That information goes into our reports, which may go into discovery in a criminal trial. The company has to stop and think and maybe ask its board and shareholders if this is something that it wants to pursue, if the objective there is really to protect the trade secret.

We met a couple of months ago with representatives of 16 major companies, the chief information officers, and we talked about these issues. We have got to do things to further that relationship. One example just very, very quickly is the proposal that the Attorney General and the FBI has made for the technical support center. This was the result of a discussion, in fact, the discussion the Attorney General and I had with six of the major CEOs of the software industry about ways we can work on these encryption issues without passing legislation which, of course, the industry is very concerned about.

And the CEOs—and we were delighted at this response—offered to not only give services but even lend us some of their scientists to work in a center where we could solve some of these problems on a case-by-case basis.

Senator GREGG. Do you need a counter-encryption center?

Mr. FREEH. Yes, we do, absolutely. This was an example of where the industry and the Government in an area of great sensitivity could work together. The Congress, in fact, passed a statute in 1998, part of the Intelligence Authorization Act, which would allow those companies to give the Attorney General those services. It would not be prohibited as a gift. So these are the kinds of initiatives that have to be pursued.

CONCLUSION

Senator GREGG. Thank you. Rather than take any more of your time because you have been extraordinarily generous with it this morning, I do intend to send some specific questions for the record to you. Especially how have the CERT teams evolved? Also, how is the evolution of the National Infrastructure Protection Center and the money that we have put into that? I would also like to get an outline of how we would approach developing a 5 year plan in this area for law enforcement. But if the Commerce Department is so inclined, I would be interested in getting a 5-year plan for how we address a coordinated effort in the areas that are not law enforcement dominated so we can have some coherence in this. You are going to get us language on the law changes you think you need?

Ms. RENO. Yes.

Senator GREGG. Statutory changes. And we are going to try to put in the Title 5 extension. Obviously, that will be a priority for this Committee. It was a priority getting it. We certainly do not want to see it lapse. I did not realize it lapsed in September. I sure hope we can get this bill signed by September. That would be a first, and it would be nice.

I appreciate all your time. This is the beginning of a road that is going to have a very long, and I suspect, many turns and forks in it. But it is a process which requires a lot of public vetting, and I appreciate your taking the time to participate in that process today. Thank you very much.

NEED FOR UNIFORM STANDARDS

Ms. RENO. Mr. Chairman, I would just like to put one other point at issue because I think it is going to be vital as to how law enforcement responds. We are going to have to develop, and I would like to work with you on it, a means of ensuring uniform standards with respect to equipment and technology. It is becoming obsolete practically before we get it installed and the cost can be astronomical or we can work with industry to develop common standards that people can understand. That will not address the issue where a vital new piece of equipment has come into play, but the costs are going to be something that needs your yankee frugality to address.

Senator GREGG. Well, I think that is a critical issue, and there are a lot of issues where we have not really gone in depth. Encryption is just a huge issue. The Director alluded to that, and it has to be resolved, as the Director said. Obviously, the purchasing of technology and keeping the Government up to speed while making sure that it is consistent is important, as you have outlined. That item and the personnel item are going to take money. I will tell you that from my standpoint, this committee has always put an extraordinary high priority on the issue of terrorism, cyberterrorism. And we are going to put the same type of priority on the issue of funding initiatives in the Internet areas that are not necessarily terrorism related but are commercially related. So I think we will be able to find the dollars, but I want to make sure they are spent effectively and in a coordinated manner. Thank you very much. I appreciate your time.

Ms. RENO. Thank you for your leadership, Mr. Chairman.
Mr. REINSCH. Thank you.

INDUSTRY PANEL

STATEMENT OF ROBERT CHESNUT, ASSOCIATE GENERAL COUNSEL, EBAY

Senator GREGG. We begin the second panel here, and I appreciate the tolerance of the second panel in waiting to testify. If the members of the second panel could come forward and take a seat, that would be very helpful. Please take a seat, gentlemen.

The second panel are members of industry. They are not representative of all the industry, obviously, but a portion of it. You will hear from Robert Chesnut, associate general counsel of eBay, which was one of the companies that was subjected to an attack last week. He will address Internet security issues, as will Mark Rasch, the senior vice president of Global Integrity Corporation. He will testify also relative to his previous experience in prosecutions of major Internet cases, specifically the Morris worm case. And finally we will hear from Jeff Richards, executive director of the Internet Alliance, which represents major Internet providers like AOL. Mr. Richards will discuss the industry's concerns about Internet security efforts, and specifically, the coordination of law enforcement agencies. Again, I thank you for your willingness to be here today and participate in this hearing.

As I think was made clear not only in my opening statement but in the comments by the members of the government, we consider the private sector's views on this to be the dominant views. This is an area where the law enforcement agencies come in, but they come in in a secondary capacity in many instances and, therefore, your ideas and opinions are important to us.

Mr. Chesnut, I appreciate your coming. I am a user of your site on a regular basis. I have a lot of New Hampshire memorabilia from eBay. In fact, if you come to my office and go to what we call the "moose room," you will see a number of things that were eBay purchased. So I am a big fan of your organization, and I appreciate your taking the time to come by. We will start with you and then go right down the line.

Mr. CHESNUT. Thank you, Mr. Chairman. eBay greatly appreciates the opportunity to come here today and to participate in this hearing. My name is Robert Chesnut, and I am the associate general counsel of eBay and prior to joining eBay last year, I was an Assistant United States Attorney here in the Eastern District of Virginia and handled a variety of cases involving computer crimes and violent crime and espionage. Since I have been at eBay, I have been able to work on some of these areas involving a partnership between law enforcement and the private industry that have already been discussed earlier in this hearing.

In 1995, as the Chairman knows, eBay created the first on-line trading community on the Internet, and today we are the world's largest e-commerce site with nearly four million items for sale at

any given time in about 4,000 different categories. Everyday we have approximately 500,000 items that are placed on our site from our over 10 million users including, I think, about 50,000 from your State.

Being the world's largest e-commerce site poses a number of challenges for us and not the least among these challenges is really a daily challenge of dealing with the protection of our web site from abuse, from hackers, database pirates, and various pranksters. As, Mr. Chairman, you know, last week we were one of the victims in the attack along with Yahoo!, e*Trade, CNN and other well known e-commerce sites. And at eBay, as the chart there shows, we were attacked at about 3 o'clock in the afternoon on February 8. The attack blocked legitimate access to eBay's site for approximately 90 minutes before we were able to turn it back. The attack continued on for another 90 minutes after we had successfully dealt with it.

That attack was followed by a second attack the following day at about 5 o'clock in the afternoon, and we were able to deal with that attack within just a few minutes without any significant disruption to our service. Mr. Chairman, the attacks are obviously extraordinarily serious. They fundamentally disrupted business on our Nation's key e-commerce sites for several days. They affected not only eBay's business but a number of—literally hundreds of thousands of individuals depend on eBay as their livelihood and so when eBay is down or blocked, they cannot do business. And so it fundamentally disrupts business all across the country when a site like ours is blocked.

Although we do not know yet who was behind the attack, it was obviously well planned and aimed directly at leading commercial web sites, such as ours. As we understand the facts, nefarious computer code was placed into computers of unsuspecting individuals and institutions, such as the University of California at Santa Barbara, and these computers were then used to launch a sustained attack on the leading web sites. The purpose of the attacks in this case was to block access to at least a portion of the web sites by bombarding them with a huge volume of traffic—what is known as ICMP traffic, Internet Control Message Protocol traffic.

In this case, Mr. Chairman, they bombarded eBay with approximately one billion bits per second of traffic, nearly double our normal incoming traffic, and this flood of what we call bad traffic effectively blocked any legitimate traffic from reaching our home page for about 90 minutes. Now since Yahoo! had been attacked the day before on February 8, we had already begun to prepare several countermeasures in case an attack like this occurred at eBay, and when the attack occurred, we took several steps to try to fight back immediately. We put some of our own firewalls into place to try to repel the attack, but the volume of the traffic was simply so heavy that the firewalls were not effective.

We quickly got in touch with our Internet service providers, and it was their lines that were actually providing the bad traffic to us, and we worked with these Internet service providers to put some filtering mechanisms in place, to try to filter out the traffic before it even got to our site. Within 90 minutes, these filters were effective in blocking the traffic and allowed our site to return to normal

usage even though the attack continued for another 90 minutes after the filters had taken effect.

It was because of those filters and because of the measures that we had taken on the eighth that when the next attack occurred at about 5 p.m. on the ninth, we had already worked with the Internet service providers; we had put some permanent fixes in place, and therefore the attack the next day was much, much easier to deal with. We were able to deal with it within just a few minutes.

The attack in this case was not distinguished by its sophistication. I think, as was mentioned earlier, this was an attack that could have occurred several years ago in terms of sophistication but what marked it was its sheer volume which was unlike any other attack that eBay had previously been a victim of. On an ordinary day, our outbound traffic exceeds inbound traffic by about a ten to one margin. That is because users are coming in asking for data from our site and we are sending a lot more out than we usually get in. Because of the huge volume of traffic, the bad traffic in this case, the incoming traffic actually equaled our outbound traffic which was an extraordinary event for us.

In our view, these sort of computer intrusions and attacks on commercial web sites are serious crimes that merit a forceful response and many of these crimes are widely viewed within the hacking community as little more than pranks. They are much more serious in our view, and they demonstrate the need for some forceful action.

Now prior to last week's attacks, eBay had already established a relationship with the computer intrusion squad at the Federal Bureau of Investigation in northern California near where our offices are located. We had already been speaking with the United States Attorney's Office in that district to work with them in the event of problems like this. eBay has recognized that the most effective way to combat cybercrime, whether it is by fraud or by hacking, is to work cooperatively with law enforcement, and we are, as a company, very comfortable in working with law enforcement in this area.

Therefore, last year, we had already set up procedures, put them in effect, so that we would be able to quickly notify the FBI in case an attack like this occurred, and as a result of that preparation, we were able to contact the FBI pretty quickly once the attack occurred to notify them of the attack and to provide them with some information that we hope will assist them in their investigation. And in the aftermath of the attack, we have also come across other leads that we have been able to quickly reach the FBI and provide them with the information.

We do believe that this attack illustrates the challenge faced by law enforcement in the investigation and prosecution of cybercrime and the importance of ensuring that the Justice Department is adequately funded to meet this challenge. The Internet has become the backbone and life blood of our new world economy, and it is imperative that consumers retain the highest degree of confidence in its reliability and security.

High tech has to take the lead. You know leading high tech companies can work cooperatively together and meet many of the challenges that are posed by cybercriminals. But industry alone cannot

solve the problem. We cannot go out and do the criminal investigations and the prosecutions of these cases. We need a partnership with law enforcement. And an important element in fighting this sort of cybercrime is ensuring that law enforcement both understands the technology and has the tools to work with private industry in investigating these crimes.

The need for an effective Internet law enforcement presence is particularly important in areas of the country that have the high concentration of high tech companies. Some examples are the Eastern District of Virginia, just right outside of the District here, northern California where eBay is located, and some other areas such as the Boston-New Hampshire corridor where high tech is concentrated. Northern California, for example, where eBay is located, has undergone a radical metamorphosis in the last 20 years. It is home now to over 6,000 high tech companies and that includes many of the leading high tech companies in the world.

This growth in the high tech industry has been accompanied by a corresponding growth in high tech crimes and these crimes are no less a threat to our economic viability than conventional crimes, but they are much more difficult to investigate and prosecute.

The areas of the country that have this high concentration of high tech companies need resources dedicated to this growing problem. In northern California, for example, the FBI's computer intrusion squad and the United States Attorney's Office must be adequately staffed to investigate and prosecute high tech related crime. Such crime is a serious issue. Computer intrusions and attacks have become increasingly frequent. They cost companies billions and billions of dollars every year to deal with, and other high tech related crimes such as theft of trade secrets, counterfeit good sales over the Internet, and simply the theft of computer equipment itself has become a major problem. According to a 1999 Rand Corporation survey, theft of high technology components such as computers costs the industry over $5 billion annually. The Justice Department cannot hope really to keep up with this high volume of work unless there are some specific resources targeted to the areas that need them with badly needed agents and prosecutors.

Likewise, it is impossible to effectively combat cybercrime unless law enforcement understands this new medium as well, at least as well as the cybercriminals do. This requires a sophisticated level of training and up-to-date computer equipment. Private industry can play an important role in this training process with law enforcement. For example, FBI has already been working with law enforcement and is providing training for law enforcement agents, for criminal agents in several places across the country, so that law enforcement understands exactly how the medium works and how the industries can actually help law enforcement and work with them quickly when crimes occur.

While this partnership can play a very important role in fighting cybercrime, it cannot be a substitute for the basic tools that law enforcement needs: agents, prosecutors, and computer equipment. eBay believes that it is important for this subcommittee to send a message to cybercriminals throughout the world that the United States Government can and will protect e-commerce from criminal activity, but if Congress is going to send a credible message that

cybercrimes will be investigated and prosecuted vigorously, law enforcement must have the resources to back up that message. We urge you to take this into consideration as you determine the appropriate funding level for these important law enforcement agencies. Thank you.

Senator GREGG. Thank you, Mr. Chesnut.

[The statement follows:]

PREPARED STATEMENT OF ROBERT CHESNUT

My name is Robert Chesnut, and I am the Associate General Counsel for eBay. Before joining eBay last year, I served for 11 years in the United States Justice Department as an Assistant United States Attorney for the Eastern District of Virginia, where I prosecuted a variety of criminal cases, including violent crimes, computer crimes and espionage matters, such as the Aldrich Ames spy case.

In 1995, eBay created the first online person-to-person trading community on the Internet. Today, eBay is the world's leading e-commerce web site with nearly 4 million items for sale in over 4,000 categories ranging from coins and stamps to toys and antiques. Every day, users around the country and the world list approximately 500,000 items on our site to sell.

Being the world's leading e-commerce web site poses a great many challenges for eBay. Not the least among them is the daily challenge of protecting our web site from attack, abuse and misuse by hackers, database pirates and pranksters.

As you undoubtedly have heard, last week eBay, Yahoo, e*Trade, CNN and other well known e-commerce sites were victims of an insidious organized attack that shut down portions of their web sites. At eBay, the principal attack occurred at approximately 3 o'clock on February 8th and blocked legitimate access to eBay's site for nearly 90 minutes. That attack was followed by a second attack on our site the next day, which we were effectively able to fend off within a few minutes.

Let me explain why these attacks are so serious. This attack fundamentally disrupted business on our nation's key e-commerce sites for several days. Although we don't yet know who was behind this attack, it was obviously well planned and aimed directly at leading commercial web sites, such as ours. As we understand the facts, nefarious computer code was serpitiously planted in the computers of unsuspecting individuals and institutions, such as the University of California at Santa Barbara. These computers were then used to launch a sustained attack on leading web sites. The purpose of the attack was to block access to portions of these web sites by bombarding them with a huge volume of what is known as ICMP (Internet Control Message Protocol) traffic. This attack bombarded eBay with over 1 billion bits per second of bad traffic, nearly double eBay's normal incoming traffic. This flood of bad traffic effectively blocked legitimate traffic from reaching our home page.

Since Yahoo had been attacked the day before, eBay had already started to prepare several countermeasures. When the attack began, we quickly took a number of steps to fight back. Initially, we put in a number of our own fire walls to repel the bad traffic, but the volume of that traffic was so heavy that the fire walls were ineffective. Quickly, we turned to our Internet Service Providers ("ISPs"), whose lines were bringing this bad traffic to our site. We worked with these providers to develop filtering mechanisms to prevent bad traffic from even reaching our site. Within 90 minutes, the filter effectively stopped the bad traffic and allowed our site to return to normal service, even though the attack itself continued for an additional 90 minutes.

The next day, a similar attack was launched against eBay at about 5:30 p.m. With our experience from the previous day and with a number of countermeasures already in place, eBay and its ISPs were able to quickly repel this attack without any disruption of eBay's services.

Let me be clear, this attack on our site was distinguished not by its sophistication, but by it sheer scale. On an ordinary day on our web site outbound traffic exceeds inbound traffic by a 10-to-1 margin. During this attack we noted that inbound traffic was so heavy that it actually equaled outbound traffic.

It's our view that computer intrusions and attacks on commercial web sites are serious crimes that require a forceful response. Although these crimes are widely viewed within the hacking community as little more than pranks, they are much more serious, as last week's attacks demonstrate.

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 com-

bat cyber crime, 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.

We believe that this latest attack illustrates the challenge faced by law enforcement in the investigation and prosecution of cyber crime, and the importance of assuring that the Justice Department is adequately funded to meet this challenge. The Internet has become the backbone and lifeblood of the new world economy. And it is imperative that consumers retain the highest degree of confidence in its reliability and security.

Leading high tech companies can work cooperatively together and meet many of the challenges posed by cyber-criminals. But industry alone can't solve the problem without establishing a partnership with law enforcement. An important element in fighting this kind of cyber crime is ensuring that law enforcement both understands the technology, and has the tools it needs to work with private industry in investigating these crimes.

The need for an effective Internet law enforcement presence is particularly important in areas of the country that have a high concentration of high tech companies, such as the Eastern District of Virginia and the Northern District of California. Northern California, for example, has undergone a radical metamorphosis in the last 20 years, and is now home to more than 6,000 high tech companies, many of which are the leading high tech companies in the world. This growth in the high tech industry has been accompanied by a corresponding growth in high tech crimes. These crimes are no less a threat to our economic viability than conventional crimes, and can be much more difficult to investigate and prosecute.

The areas of the country that have a high concentration of high tech companies need resources dedicated to this growing problem. In Northern California, for example, the FBI's computer intrusion squad and the United States Attorney's Office must be adequately staffed to investigate and prosecute high tech-related crime. Such crime is a serious issue. Computer intrusions and attacks have become increasingly frequent, costing companies billions of dollars each year. Other high tech-related crimes, such as theft of trade secrets, sale of counterfeit goods on the Internet and theft of computer and high tech components, also require intervention by law enforcement. According to a 1999 Rand Corporation study, theft of high technology components alone costs the industry $5 billion annually. The Justice Department cannot hope to keep up with this volume of work unless specific resources are targeted to provide them with badly needed agents and prosecutors in key high tech regions of the country.

Likewise, it is impossible to effectively combat cyber crime unless law enforcement understands this new medium at least as well as the cyber-criminals do. This requires both a sophisticated level of training, and up-to-date computer equipment. Private industry can play an important role in the training process. For example, eBay already provides regular training to law enforcement agencies to help them understand Internet commerce and the kinds of information available to assist them in finding and gathering evidence of cyber crimes.

While this partnership between industry and law enforcement can play an important role in fighting cyber crime, it cannot substitute for the basic tools that law enforcement must have to be effective—agents, prosecutors, and computer equipment.

It is important for this Subcommittee to send a message to cyber criminals throughout the world that the U.S. Government can and will protect e-commerce from criminal activity. But if Congress is to send a credible message that cyber crimes will be investigated and prosecuted vigorously, law enforcement must have the resources to back up that message. We urge you to take this into consideration as you determine the appropriate funding level for these important law enforcement agencies.

Thank you for giving us the opportunity to testify today and I would be glad to answer questions you may have.

STATEMENT OF JEFF B. RICHARDS, EXECUTIVE DIRECTOR, INTERNET ALLIANCE

Senator GREGG. Mr. Richards.

Mr. RICHARDS. Mr. Chairman, I am Jeff Richards, executive director of the Internet Alliance, and on behalf of the Alliance I want

to thank you for this opportunity. We would like to give our views on criminal activity on the Internet, on the necessity of enforcing laws applicable to that activity, and on the need for Federal law enforcement authorities to have resources that enable them to better carry out their mandate.

Since our founding in 1982 as the Videotex Industry Association, the Internet Alliance has been the only trade association to address online and Internet issues from a consumer perspective, consumer confidence and trust. The Internet Alliance's 70 plus members today represent more than 90 percent of consumer access to the Internet in the United States and our Law Enforcement and Security Council gather senior security officials—in fact, this organization is co-chaired by AOL and MCI-Worldcom-UUNET—to bridge the gaps between industry and law enforcement agencies.

We are actively then building confidence and trust and it is necessary to do that so that this becomes the global mass market medium of this century, the Internet century. So the Internet Alliance has recognized that the Internet can mature really as a revolutionary mass medium and one that is about new knowledge relationships and choices but only if we all promote the public's trust and confidence. It in the context of that trust and confidence that we assess the recent denial of service attacks.

Vandals flooded important web portals and sites with spurious requests, rendering them temporarily unavailable, as we have heard, to would-be users. For many Americans, last week's event marked their first exposure to one of the downsides of the Internet's main strengths: its relatively open architecture. Consumers could wrongly conclude that the Internet is essentially an open sieve for malcontents or criminals.

Internet vandalism has occurred before and it will occur again. Destructive, freely distributed software tools are created by those with malicious or misguided motives, and more will be created in the future. But at the same time, I think some perspective is in order. First, the duration of the interrupted service was measured in hours, not days. In an industry less than a decade old, that record compares favorably with electrical power outages during storms or telephone service interruptions. When the assault was detected, teams of experts employed additional capacity and screening tools—we have heard some of those talked about this morning—bringing the situation under control.

I just want to point out this in itself is an impressive demonstration of the sophistication and responsiveness of service and infrastructure providers. And very importantly, at the same time, industry and law enforcement agencies began cooperating on these investigations starting that very day. So my point is we must not overreact to these events. Whether in personal relationships, in the process of democratic government, or in the operation of the Internet, openness, Mr. Chairman, is always accompanied by a degree of risk. In Internet terms, though, then we say openness needs to be preserved so that small as well as large enterprises can be part of this new economy, so citizens can speak freely, and so that the web is truly a global medium.

So the effectiveness of web attacks can and will be reduced. I am confident we are going to steer the right course between security

on one side and openness and freedom on the other, and this hearing is an important one to advance both of those goals.

So at the Internet Alliance, we believe in a simple approach: first things first. With respect to crime on the Internet, that means focusing on security and on the effective enforcement of existing criminal laws. Prosecutions under such laws serve two goals equally well, deterrence on the one hand and promotion of the public's confidence in the Internet medium. Investigation and prosecution of criminal acts in the new on-line world pose new challenges for agencies that we have heard about today. And as a result, law enforcement ranges from some centers of excellence to some haphazardness to some serious lacks. I am not just referring to denial of service attacks. The situation can extend across several categories of crime.

So now I will speak more broadly and speak specifically of the Internet Alliance's support of additional appropriations for Federal law enforcement agencies, assuming that those resources will be spread among different categories. What are some of the keys to improved enforcement of existing laws in the Internet space? A short list would include training of existing officers in computer and Internet skills and application of constitutional and statutory liberties in the Internet context. It would include hiring additional experts, additional computer and other investigative equipment, and very definitely improve coordination and cooperation among law enforcement agencies themselves and with the industry. I think there has been great progress there and continuing work on jurisdictional matters. It would include public education efforts to urge consumers to act wisely and cautiously to protect themselves online as they do off-line.

Today, law enforcement is inadequately trained to investigate crimes and support effective prosecution of current laws in the Internet space. This is no indictment of law enforcement agencies. There are centers of excellence within DOJ, FBI, some State attorneys general, some State and metropolitan police forces, but only a small percentage of law enforcement agencies, perhaps 5 percent or less, in the United States have the knowledge and skills to prosecute properly received Internet related complaints, to adequately investigate those crimes and otherwise assist in the successful prosecution of Internet criminals.

We have no reason to believe this situation is better in any other nation. To help address these challenges, the IA has moved beyond rhetoric in the areas in a number of constructive law enforcement related activities and for the Internet Alliance these include training, and we heard reference earlier this morning, to work with several agencies including Department of Justice, FBI, and our Law Enforcement and Security Council where we are preparing updated law enforcement training and resource materials and a much needed secure worldwide directory of key industry and law enforcement contacts.

We must resist, frankly, overreaching, even in the name of security, and make certain the constitutional and other statutory protections in investigations and prosecutions are observed and we think that training is a critical part of achieving that.

And finally, we must also keep clear the distinction of roles between industry and law enforcement. We as companies can and will do more to help law enforcement succeed in all its duties, but industry cannot be made an agent of law enforcement as some have proposed abroad.

Let us return quickly to last week's distributed denial of service attacks. Broadly speaking, what can we learn for the future? First, we see that widespread prevention at the user end; the university that was cited, for example, the local system administrator end could have made a difference. This is a broad issue that we need to continue to address. It appears that many of the computer resources used to launch these attacks were not those of ISPs, for example, or networks or other Internet companies, but some of those end-user customers themselves. That means that all of us must be vigilant and take steps to close the backdoors, apply software patches, update firewalls, and use proper Internet hygiene.

Second, we see that the apparent advanced planning, coordination, and delayed execution of this launch-on-command attack would have evaded real time monitoring and intercepts of the Internet by law enforcement, and we do not support at this time such steps to a solution.

Third, the process of identifying and prosecuting those responsible, which will increase public confidence and deter future vandalism, would be significantly more efficient if law enforcement agencies get the financial resources that they need.

In conclusion, each of us can make valuable contributions against Internet crime. For our part, the Internet Alliance will pursue law enforcement training efforts. We are going to prototype the secure directory of industry and law enforcement contacts. We will bring forward a carefully crafted proposal regarding forgery of header and routing data and we will strongly pursue industry best practices in the areas of law enforcement and security addressing data retention domestically and internationally as an example. Industry itself will continue to develop and deploy more and more secure and stable hardware and software to improve the consumer Internet experience.

Turning to the government's contribution, we ask Congress to support the effective enforcement of current laws through increased appropriations and through ongoing oversight and encouragement. Thank you. I would be glad to answer any questions as best as I can.

Senator GREGG. Thank you, Mr. Richards.

[The statement follows:]

PREPARED STATEMENT OF JEFF B. RICHARDS

Mr. Chairman, Mr. Ranking Member and Members of the Committee, I am Jeff B. Richards, Executive Director of the Internet Alliance (www.internetalliance.org). On behalf of the Alliance, I thank you for the opportunity to give you our views on criminal activity on the Internet, on the necessity of enforcement of the laws applicable to that activity, and on the need of federal law enforcement authorities for resources that would enable them to better carry out their mandate to protect law abiding citizens and businesses from criminals.

Since its founding in 1982 as the Videotex Industry Association, the Internet Alliance (IA) has been the only trade association to address online Internet issues from a consumer Internet online company perspective. Through public policy, advocacy, consumer outreach and strategic alliances, the IA is building the trust and con-

fidence necessary for the Internet to become the global mass-market medium of this century, the Internet Century. The Internet Alliance's 70-plus members represent more than ninety percent of consumer access to the Internet in the United States. IA's Law Enforcement and Security Council brings together senior security officials of key IA members to bridge the gaps between industry and federal, state, and international law enforcement agencies. It benefits from IA's unique presence—in the fifty states, Washington and abroad—to increase its knowledge and leverage. Since May of 1999, the Internet Alliance has been a separate subsidiary of the Direct Marketing Association, bringing the resources of a 4,500-member organization to bear on Internet issues and their resolution.

The Internet Century

Coming as it did at the end of the last millennium, the sudden and exponential growth of the consumer Internet over the past ten years will undoubtedly be seen as a portent of things to come in the new "Internet Age." Less than a decade after the development of the first Web browser, billions of dollars were spent online in 1999. The range of transactions was broad indeed—from books and records to food and wine, from computers and exercise equipment to automobiles and houses, from pay-to-view webcasts and news alert subscriptions to online banking and computer training. In short, The Internet is transforming the American economy and consumerism itself.

Growing public acceptance of the Internet has important implications. For consumers, the new medium has brought a range of new options, accompanied by some new and different worries. For business, the Internet has brought new methods of reaching customers, as well as new competition from unfamiliar places. For the U.S. government, online commercial activity has created a vast new economic sector, an engine of productivity that renews many familiar challenges and generates a few new ones.

By any reasonable measure, however, the Internet has been a positive development for consumers, business and government. By most accounts, the rise of the Internet has been a key factor in the sustained economic growth of 1990s America, helping to put record numbers of Americans to work and generating productivity increases that have in turn helped buy down federal and state budget deficits, tame inflation, and create the circumstances for a record period of economic growth.

Consumer Confidence and Trust

The Internet Alliance has always recognized that the Internet can mature as a revolutionary mass medium, successfully empowering consumers through new knowledge, relationships and choices, only if it promotes the public's confidence and trust. The process of increasing consumer confidence and trust has led the Internet industry to vigorously address a range of policy issues, including privacy, unwanted commercial e-mail, information security, enforcement of the laws on the Internet, marketing to children, taxation, and international jurisdiction and consistency. Of particular relevance to the topic of this hearing, in 1999, the Internet Alliance inaugurated its Law Enforcement and Security Council, bringing together experts from leading companies to undertake concrete law-enforcement-focused projects, to regularize contacts between law enforcement and industry, to find points of agreement and join efforts with non-U.S. Internet organizations, and to work on "best business practices."

Denial of Service Attacks

Let me first add some perspective about the recent denial of service attacks reported prominently in the media beginning February 7. Vandals flooded important Web portals and sites with spurious requests, rendering them temporarily unavailable to would-be users. While I cannot comment on ongoing investigations, we take denial of service attacks seriously, both for the damage they do and for the perceptions they create. For many Americans, last week's events marked their first exposure to a downside of one of the Internet's main strengths—its relatively open architecture. Consumers could erroneously conclude that the Internet is essentially an open sieve for malcontents or criminals.

Granted, Internet vandalism has occurred before, and doubtless will occur again. Destructive, freely distributed software tools are available to those with malicious or misguided motives, and more will be created in the future.

Maintaining Our Perspective

At the same time, I think some perspective is in order. First, the duration of interrupted service was measured in hours, not days. In an industry less than a decade old, that record compares favorably with electrical power outages during storms or periods of heavy usage, and with phone service interruptions. When the assault

was detected, teams of experts deployed additional user capacity and screening tools, quickly bringing the situation under control. This is an impressive demonstration of the sophistication and responsiveness of service and infrastructure providers. At the same time, industry and law enforcement agencies began cooperating on investigations seeking to identify and prosecute those responsible.

What is new about the events of the last ten days is the level of public awareness and scrutiny. In turn, this offers us a renewed opportunity to further improve our performance. Industry must continue to develop and deploy effective technologies and countermeasures, with the Internet itself increasingly serving as a platform for solutions providers.

At the same time, we must not overreact. Whether in personal relationships, in the processes of democratic government, or in the operation of the Internet, openness always is accompanied by a degree of risk. We would not think of abandoning these benefits because of their risks—we accept risks even while trying to reduce them. Thus the goal is not to achieve perfect security at any cost; it is to find an acceptable balance, and thereafter to work on improving the terms of that balance. In Internet terms, openness needs to be preserved so that small as well as large enterprises can be a part of the New Economy, so that citizens may continue to speak freely, and so that the Web is truly a global medium.

The effectiveness of Web attacks can and will be reduced. And I am confident that we will steer a wise course between security on the one side, and openness and freedom on the other. This hearing is one important opportunity to advance both goals.

First Things First

At the Internet Alliance, we believe in a simple approach—"first things first." With respect to crime on the Internet, that has meant focusing on security and on the effective enforcement of existing criminal laws. Prosecutions under such laws serve two goals equally well: deterrence, and promotion of the public's confidence in the Internet medium. However, investigation and prosecution of criminal acts in the new online world pose new challenges for law enforcement agencies. As a result, law enforcement online ranges from haphazard to nearly nonexistent. Our Federal agencies have led the field, developing the most skilled corps of professionals and the greatest depth of experience in the world. But unless they get additional resources, they will be unable to enforce federal laws properly and will have little capability to help upgrade state and local agencies.

I am not referring just to denial of service attacks. The situation extends more or less across all categories of crimes. Thus, the remainder of my comments will speak more broadly, and the IA's support of additional appropriations for Federal law enforcement agencies assumes those resources will be spread among different categories according to need, urgency and the degree of improvement expected in each.

What are some of the keys to improved enforcement of existing laws in the Internet space?

A short list would include training for existing officers in computer and Internet skills, and in the application of constitutional and statutory civil liberties in the Internet context. It would include additional computer and other investigative equipment, and the hiring of additional personnel to investigate and prosecute Internet crimes, as well as to improve coordination and cooperation among law enforcement agencies themselves and with the Internet industry, continuing work on jurisdictional matters. And it would include public education efforts to urge consumers to act as wisely and cautiously to protect themselves online as they do offline.

Today, law enforcement is inadequately trained to investigate crimes and support effective prosecution of current laws in the Internet space. This is no indictment of law enforcement agencies. There are some centers of excellence within the Department of Justice and the Federal Bureau of Investigation, some state Attorneys General offices, and a few metropolitan police forces. However, only a small percentage, probably well under five, of law enforcement agencies in the United States have the knowledge and skills to properly receive Internet related complaints, adequately investigate those crimes through online and offline resources, develop and maintain admissible evidence, refer complaints through the system, network with experts, and otherwise assist in the successful prosecution of Internet criminals. We have no reason to believe the situation is any better in other nations.

And superimposed on the challenge of adding personnel and upgrading skills and equipment is the evolving nature of the Internet and the speed of action the new medium makes possible. Today, law enforcement too must move on "Internet time," and that takes prioritization, continual training and management focus.

Finally, the nature of the Internet requires us to seek a wise balance among local, national, and international law enforcement, especially as we negotiate the ground rules of this first global medium. We know that today citizen complaints may enter the system at any level of jurisdiction. The Internet is simultaneously intensely local and intensely global. The Internet will be a vehicle—one among many—for the commission of criminal acts within communities. The IA tracks state laws, and we know that in this state legislative cycle, we may see more than 2,200 Internet-related bills. So at least in the foreseeable future, the Internet and law enforcement will be intertwined at far more than the federal level.

Concrete Steps Going Forward

IA has moved beyond rhetoric in a number of constructive law-enforcement related activities. These include:

Training

In coordination with several agencies, including the Department of Justice and the FBI, the Internet Alliance's Law Enforcement and Security Council is preparing updated Internet law enforcement training and resource materials. While many of our members already provide briefings, materials and consultations for the law enforcement community as requested, needs may soon outstrip individual companies' capabilities. By combining our experience, the IA can provide both basic introductory and updated, advanced materials to increase law enforcement's expertise and success. This is a commitment we undertake knowing that industry's roles are distinct from those of law enforcement, but that we can help each other where they converge.

Coordination

Cooperation among law enforcement agencies is another basic aspect of a "first things first" philosophy. Again, we applaud the leadership of those who have built expertise and a track record of successful enforcement and prosecution. We also believe that since the Internet has grown so quickly, it has now outstripped the often "ad hoc" communications among agencies. We encourage law enforcement at all levels to share techniques and their own "best practices" rapidly and thoroughly.

IA recognizes that coordination among international enforcement agencies is necessary to adequately fight crime on the borderless Internet. In September of last year, IA assumed a leadership role at an international conference of enforcement agencies in Vienna, Austria, for the first time catalyzing a constructive business/government dialogue on tackling specific Internet crimes.

Domestically, we are giving input to the FBI, at its request, in the development of reporting mechanisms for the new Internet Fraud Reporting Center. In another initiative we respond to the fact that the Internet industry itself has not always been easily accessible to law enforcement. Accordingly, in conjunction with DOJ's recently announced "24/7" computer crime personnel network, the Internet Alliance's Law Enforcement and Security Council is prototyping a secure online directory of law enforcement and industry contacts. By consulting this list, law enforcement officers will quickly identify and be able to contact designated individuals within Internet companies who are responsible for responding to their requests.

We firmly support the appropriation of new federal dollars to bring enforcement of current laws into the Internet Century. As new resources are made available, the continuing challenge will be to apply them optimally, and to make certain that this financial commitment is not merely a short-term focus for policymakers, nor on the other hand, a platform for front-line monitoring of Internet activities generally. Priorities should be clear and rational. We need to include local and international law enforcement, industry and problem-solving organizations such as ours. Our consumers, and your constituents, should expect nothing less.

Forging Header and Other Routing Information

Based on our industry experience, the Internet Alliance believes that one tightly tailored legislative approach would be useful in diminishing distributed denial of service attacks, as well as a fundamental problem affecting consumers and ISPs—unwanted commercial e-mail sent through forged header and other routing information. We value the Internet's open architecture and we value commercial and other speech. We also see that both are undermined by the deliberate forgery of key message header and routing information. We will soon offer to Congress a tightly focused legislative proposal aimed at these forgeries. We believe that it will preserve the benefits of the Internet to millions of consumers and to our economy while making criminal the act of forging these important technical data upon which the Internet infrastructure relies.

Resisting A Crisis Mentality

The recent denial of service attacks may lead to calls for new laws and new police powers. We respect the motives for these calls, but we have serious misgivings about responding quickly, and we urge this Subcommittee and the Congress to exercise caution and scrutiny. When current law is not sufficiently enforced, there are numerous risks in pursuing new ones. We must build the solid track record of enforcement in the current environment before we can accurately determine what further steps are needed. We must not pass laws of dubious enforceability, risking erosion of the public's confidence in law enforcement and in the Internet. We must resist overreaching, even in the name of security, and make certain that constitutional and statutory protections in the investigation and prosecution of Internet crimes are observed.

The world is watching the United States carefully. There are nations who would like to exercise control over Internet traffic and content, curtail U.S. innovation and global opportunities, and bend technical advances to their own purposes. Our national policy has been to resist these developments through negotiation, persuasion and example. Action by Congress to grant new powers to law enforcement to monitor or control Internet activities will be cited by these nations to undermine U.S. moral authority and to justify their own activities.

We are wise instead to ensure that our traditional criminal law restraints and balances are carried over into the Internet context. We are wise to invest and prioritize wisely, and to build international cooperation based on well understood legal and law enforcement principles. And we will all build consumer confidence and trust through making clear our governments' enforcement and prosecution prowess, rather than communicating encouragement of additional government surveillance of citizens. At a time when concern about privacy is intense both in the U.S. and Europe, we risk too much by appearing willing to skip over the fundamentals. Basics should indeed come first.

We are also on solid ground when we keep clear the distinction in roles played by industry and law enforcement. For industry, the influence of the marketplace is overwhelming. Increasingly, companies will be scrutinized and judged by consumers on their security practices and their investments in technology advances. Companies and associations of companies have done and will do more to give consumers a reliable, satisfying and productive Internet experience than any other sector of society. They can and will do more to help law enforcement succeed in its duties. But industry cannot and must not be made an agent of law enforcement, as some have proposed abroad.

Lessons Learned

Let's return to last week's distributed denial of service attacks. Broadly speaking, what can we learn for the future? First, we see that widespread prevention at the user end—the local system administrator end—could have made a difference. Generally, we promote the idea that security must be a high priority for all entities connected to the Internet. This means not only commercial backbone and access providers and web site hosts and merchants, but also not for profit and other providers and users. It appears that many of the computer resources used to launch the attacks were not those of ISPs, networks or other Internet companies, but in fact "end users" themselves. This means that all of us must be vigilant, and must take steps to close "back doors", apply software patches as they become available, update firewalls and use proper Internet hygiene. In the coming days and weeks, you can expect that many of us in the Internet community will be proposing specific recommendations about system administration, especially as details surrounding the attacks are made clear. Second, we see that the apparent advanced planning, coordination, and delayed execution of the "launch on command" attacks would have evaded real time monitoring and intercepts of the Internet by law enforcement, and do not support such steps as a solution. Third, the process of identifying and prosecuting those responsible for the attacks, a process which will increase public confidence in the Internet and hopefully deter future Internet vandalism, would be significantly more efficient if the federal law enforcement agencies had the financial resources they need.

Conclusion

Each of us can make valuable contributions in the fight against Internet crime.

For its part, the Internet Alliance will pursue its law enforcement training efforts. We will prototype the secure directory of industry and law enforcement contacts. We will bring forward a carefully crafted proposal regarding forgery of header and routing data. And we will strongly pursue industry "best practices" in the areas of law enforcement and security addressing matters such as data retention domestically

and internationally. Industry itself will continue to develop and deploy ever more secure and stable hardware and software to continually improve the consumer Internet experience.

Turning to the government contribution, we ask the Congress to support the effective enforcement of current laws through increased appropriations and through ongoing oversight and encouragement.

Thank you. I will be glad to answer any questions to the best of my ability.

STATEMENT OF MARK RASCH, VICE PRESIDENT, CYBERLAW, GLOBAL INTEGRITY CORP.

Senator GREGG. Mr. Rasch, I understand you are with Global Integrity, and we would appreciate any comments you might have.

Mr. RASCH. Yes. Good morning, Chairman Gregg. Thank you for inviting me to testify today on the important issue of Internet security. I am Mark Rasch, and I am vice president of Global Integrity. We are a subsidiary of Science Applications International Corporation, and we are located in Reston, Virginia. What we do is we work with banks and Fortune 100 companies along with Internet companies, dot-com companies and the like, and help them develop secure architectures. We help them respond to computer security incidents, and we help them monitor their firewalls and things like that dedicated to information protection.

Before I joined Global Integrity, I was a trial attorney with the Fraud Section of the Criminal Division of the Justice Department responsible for investigating and prosecuting computer and high technology crimes. Among the cases I worked on were the investigation and prosecution of Robert Morris, the Cornell University graduate student who created a computer worm back in 1988 that shut down 10 percent of the computers on the Internet. At that time, that was about 6,000 computers. There are probably more than that right now in a three square block radius in Concord, New Hampshire.

I also worked on the investigation and prosecutions of the *Cuckoo's Egg* cases. That was a case involving foreign espionage against the United States by computer and the investigations of Kevin Mitnick, a hacker who was recently released from jail in California.

At the time I left the Justice Department in 1991, the Computer Crime Unit consisted of me on a part-time basis. Right now, the Computer Crime Unit has a Computer Crime and Intellectual Property Section of the Justice Department which has more than 18 attorneys and that number continues to grow.

As you requested, I would like to address three principal topics today. First is the nature of the threats against the infrastructure, particularly the commercial infrastructure, the vulnerabilities and trends that we have seen in cyberspace. Second, I would like to address what the private sector is doing and can do in the future on its own to help protect the critical infrastructure. And the third thing is the proper role of law enforcement and the role of the government in general in helping to protect and defend cyberspace.

The distributed denial of service attacks last week against these companies here have made painfully clear that there are very few rules in cyberspace. Information security has to a great extent been the stepchild of electronic commerce. For America to remain competitive and foster the growth of electronic commerce with its increases in productivity and convenience, it is essential that we pro-

tect the critical infrastructure. The gravamen of the situation is essentially this. There are genuine threats to electronic commerce and privacy and security of digital information, but none is so significant that they should long deter us from continuing on the path towards the growth of electronic commerce.

The same Internet that empowers a single individual to obtain a lower interest rate on a home mortgage or buy something from eBay at a lower price also would empower someone from a basement or garage in Concord, New Hampshire to get information about a transaction in say Charleston, South Carolina, or break into a dot-com business in Palo Alto, California. The Internet is no respecter of borders or sovereignty. Government, in general, and the U.S. Government in particular, does have a legitimate role in helping make the Internet more robust, more secure, and more dependable by helping design more dependable computer systems.

But the government should not use the general insecurity about online commerce as an opportunity to take upon itself new powers of investigation, new powers to compel cooperation or reporting or new opportunities to increase the regulatory burden on those doing e-business. The government can, though, do more to be a partner with e-business with the commercial sector and to promote trust and confidence in its abilities and its dedication to security.

First question is, of course, is the sky falling? And the answer to that is maybe. What we see from last week's attacks against these various electronic companies is essentially a wake-up call, but it is not the first wake-up call. We have had a series of wake-up calls that have shaken the industry and said we need to do something about security. I want to emphasize the fact that none of the sites mentioned here were actually hacked themselves. What actually happened was these automatic programs monitored the networks and then broke into other people's sites using known vulnerabilities, widely known, widely publicized vulnerabilities.

Had those vulnerabilities been effectively fixed by the sites that were broken into, this attack could not have taken place. So if we can fix the problems we know about, we will be 90 percent of the way there. Cybercrime represents a real and growing threat although it is difficult to measure its scope. Reporting of cybercrime is limited by virtue of the difficulty in detecting it, and, in fact, a study that was done by the Air Force indicated that fewer than 9 percent of cybercrimes are ever even detected, much less reported, much less investigated, much less prosecuted.

So there is another problem as well and that is the understandable reticence, especially in the commercial sector, to report cybercrime because of the nature of electronic commerce being dependent upon not only security but also on confidence.

We did detect the following trends over the last year, however. First of all, distributed attacks, the type that we have seen here last week, specifically indicated by the activities of late 1999 and last week, are increasing. Compromising the same vulnerabilities in systems is the predominant method of attack. Hackers use the same old tricks that they have been using for years to break in. Most incidents and penetrations seem to be crimes of opportunity. Although there may be significant planning involved in them, they break in where they feel they can break in.

The release of point and click tools—these are complete programs that are available on the Internet that you can download—have made it easier for teenage hackers and others to simply download programs and break into people's computers. These can be perpetrated by what we call "script kiddies" who download the tools and more sophisticated hackers can take these same tools and alter them. I would guess that the types of attacks we saw last week could be perpetrated again next week if somebody simply altered the programming and made them appear somewhat different.

Generally speaking, attack coding has become more sophisticated, and it has been very creative. Media exposure seems to be at least one of the catalysts for many of the attacks and appears to correlate to web attacks and hacks. These are attacks on people's web sites. Organizations appearing prominently in the news or those launching new advertising campaigns or IPOs tend to be the ones that seem to be the targets of many of these hackers.

Also, the electronic workplace has bred a certain degree of disloyalty among employees. Because they work and take a more independent and individual view of their job and their work and because of the emergence of these dot-com millionaires and the IPO frenzies and the ease in starting one's own business, there is a tremendous amount of competition to obtain intellectual property. As a result, we see sophisticated attacks against computer systems in order to steal intellectual property which then can be utilized in competition with other companies.

We live in a world where more information that is more connected and is more sensitive is contained on more computers. Those computers are more connected to each other, more vulnerable to attack, and, therefore, we need to take electronic commerce security extremely seriously.

Now, the next question is what is the private sector doing, and how can they do more? It is difficult to generalize about an entire industry, particularly an industry that is moving as quickly as the e-commerce industry is moving. Some commercial enterprises, particularly in the banking and financial services industry, which have a tradition of security, have taken the problem very seriously. Newer e-commerce companies like eBay, where security is perceived to be important, have taken tremendous steps as well.

On the other hand, there are companies out there, and thousands of them, where there is a competition for resources and where they have a choice of promoting more functionality or more security, they may choose the easy route and take more functionality. And, therefore, the institutions like banks, brokerage houses, and insurance companies are generally well secured. They have done a number of things in the past several years to help promote even increasing security. I would like to speak about two of them right now.

As a result of Presidential Decision Directive 63, PDD–63, the Commerce Department, the Securities and Exchange Commission, and other areas of the government have promoted a private enterprise of cooperation among the financial services industries called the ISAC. This is the Information Sharing and Analysis Center, and the FS, or Financial Services ISAC acts as a clearinghouse of information about information security threats, vulnerabilities, and

incidents, and so what the FS ISAC does is it acts as a mechanism for these disparate companies to share information on a real-time basis about attacks that are going on.

One of the problems is that companies do not like to report these types of incidents for a variety of different reasons. What the FS ISAC allows them to do is to share the information in an anonymous and confidential and secure manner. That is just one of the things that the financial services industry is doing to help make themselves more secure.

Another thing is the Banking Industry Technology Secretariat, or BITS, which is a group of various banks and other financial institutions, has formed something called the BITS Laboratory. What the BITS Laboratory does is it will test any products, whether it is hardware or software, biometric devices, bill payment systems, operating systems, e-mail systems and the like, against a set of common criteria. They establish a set of criteria, and this is run by Global Integrity, and then the products get to be tested against that criteria and get essentially what amounts to the Good Housekeeping Seal of Approval.

Once the product is then tested and cleared for the security criteria, then other banks and financial institutions can buy these products with a reasonable degree of confidence and belief that the product is reasonably safe. What this eliminates is the possibility that products get shipped to banks or financial institutions with default settings that are insecure. Essentially we would run the same types of hacker tools against these products that the hackers would to test them before they get into the banks or financial institutions.

Now no method of security is going to be 100 percent effective. But these are some of the mechanisms that at least the financial services industry, which represents about 70 percent of the work that we do, are doing to protect themselves. This model of information sharing within the FS ISAC is going to be perpetrated against other of the critical infrastructures. Another model is the National Secure Telecommunications Advisory Commission or NSTAC that acts in a similar capacity for sharing information about vulnerabilities in the telecommunications industry. So we will see similar types of ISACs that are going to be developed in the energy sector, in the telecommunication sector, the power sector, and other sectors as to that.

Now, the next question is what is the role of law enforcement and the appropriate role of law enforcement? There has been a lot of debate about that. Just as protecting the highway system is not the exclusive role of the police department, protecting the information superhighway is not exclusively or even primarily the role of law enforcement. Law enforcement's role is, in fact, that. It is to enforce the law, to arrest offenders, to investigate criminal activity, but it need not be only reactive. It has a proactive role as well.

Just as in the Nation's highway system, the Department of Transportation, for example, does highway planning to make sure that the roads are safe, to set standards for trucks and cars and vehicles on the highway, I think that the government has a legitimate role in setting standards and helping to set standards for security and for interoperability on the information superhighway.

However, one of the problems we have is a fundamental distrust between the commercial sector and law enforcement. This is not to say that eBay is not going to be calling the police or the FBI when they get hit by an attack or things like that because by and large I found that the commercial sector wants to do the right thing. They want to report criminal activity. They want to know who to call, and they want to work cooperatively.

I have also found that law enforcement, by and large, wants to work cooperatively with the commercial sector. However, what we find is, for example, if you are buying a commercial encryption product that has been "approved," and I use that term in quotes, by the National Security Agency, there will be a perception in the commercial sector that that product has been in some way deliberately weakened and, therefore, there will be a fundamental mistrust of it.

That problem is also emphasized in the area of incident response. By and large, as I said, the commercial enterprises want to do the right thing and call the FBI or call the Secret Service when there has been an incident. However, one of the things that you find is that when there has been an incident, there is a reluctance in the commercial sector to call law enforcement because they are afraid of losing control over the investigation, losing control over their resources. There is a concern that the FBI might come in there and say, "tell me what was the computer that was hit?" You would point to a particular computer and say, "that is our main server that is serving all of our Internet traffic, that was what was hit." And the FBI will say, "well, we need that for evidentiary purposes," and walk away with a handcart and your main server.

So we need to have better coordination and education between the commercial sector and between the FBI and other law enforcement agencies so that they each understand each other's positions, and so they are each more sensitive to each other's positions as well.

So we see one of the problems is a problem of simple cooperation, coordination, and communication. We need to do more of both in the commercial sector and in the law enforcement sector to promote that. One of the problems is that to the FBI and law enforcement, a successful case is when there is a public attack on a site and they are able to arrest a non-juvenile defendant, have a swift and public prosecution, resulting in a conviction and a sentence which will act as a deterrent both to that individual and to others as well.

However, in many cases to the private sector such a result would be disastrous. The public nature of the trial would reveal the very vulnerabilities that were used and exploited to attack the system in the first place. It would result in a decrease in confidence by the public in electronic commerce in general and in security. So, generally, we have found that companies that have reported computer security incidents lose anywhere from 10 to 100 times as much money as a result of the reporting, and the public nature of that reporting, than they lost in the actual attack itself.

Additional problems plague law enforcement agencies as well. It is difficult, if not impossible, for them to train and retain staff skilled in the subtleties and nuances of new high technology crime scenes. The pace of technological change coupled with the lure of

the private sector may discourage all but the most dedicated staff from remaining within law enforcement. Law enforcement is also used to dealing with other law enforcement agencies in coordinating criminal responses.

In the new Internet era, however, the primary investigators are no longer those with badges and guns. Computer crimes are initially investigated by the 23-year-old system administrator who happens to be on duty at 4 o'clock in the morning. That is the person who is investigating the computer crime. Then they call the IT professionals who call the legal staff within the company who then call the security staff within the company, and, eventually, law enforcement may be called.

So when law enforcement, the Federal law enforcement agencies, are training and helping train the State law enforcement agencies as being the quote "first responders" to the crime scene, by the time the law enforcement gets called in any capacity, they are already down to the 20th or 30th respondent. So we need to do more to train commercial enterprises about how to collect and manage evidence for the purposes of later prosecution.

Add to this the problem of the fast pace of change of both law and technology, differences in rights to privacy in various countries, the inability of any individual law enforcement agency to act beyond its borders, and the transnational nature of computer crime, and we are left with serious impediments to relying upon law enforcement as a means of prevention of computer crime.

There are a few things that I mentioned in my prepared testimony that law enforcement does need to do and that the government needs to do. Among these are helping to set standards working with NIST, working with the commercial sectors, working with companies like Cisco and IBM, to help set standards for the Internet and for Internet security; to help fund additional research and development into security protocols; letting the commercial sector be part of the development of the laboratory facilities; letting the commercial sector both get training and give training to law enforcement agencies; additional funding for education and training, not just at colleges and universities but also specialized training for law enforcement and for the commercial sector.

Providing additional technical support to companies both within law enforcement and within the Department of Commerce; promoting new security technologies both as a consumer and as a developer of security technologies; and most important, the government needs to lead by example. The government needs itself to protect its own critical infrastructure, develop new technologies and new methodologies to protect itself, and then share these technologies with the commercial sector.

Finally, there are some things that the government should not do. The government should not seize the publicity surrounding these recent attacks to take upon itself new powers or new regulations or impose new burdens on those operating in the web. Any such regulations are likely to be ineffective, counterproductive, and impose a disproportionate compliance burden on U.S. companies.

The government must respect the fundamental rights to privacy, including a respect for anonymity where appropriate. For political and social discourse to flourish on the web in America and abroad,

governments must agree not to unduly burden the privacy rights of the electronic community. The government should not use the legitimate threats to computer systems as a justification for increased monitoring or surveillance of its citizens or of others. While much of the traffic on the Internet is public in the sense that the IP traffic is transmitted over public networks, the government should not create a database of normal traffic patterns or surveil otherwise innocent Internet traffic.

Most importantly, the government should not rush to pass new laws or new regulations unless and until it has demonstrated that current legal regimes are both inadequate to solve the problems and are not preserving other fundamental rights or liberties. We should not sacrifice liberty at the alter of security.

The final question is whether or not we need new laws?

Senator GREGG. Unfortunately we are running out of time here. Can we take that in your submission, Mr. Rasch?

Mr. RASCH. Yes. Thank you, Mr. Chairman, and I will be glad to answer any questions you might have.

[The statement follows:]

PREPARED STATEMENT OF MARK D. RASCH

Good morning Chairman Gregg, Senator Hollings, and members of the Subcommittee. Thank you for inviting me to testify today on the important issue of Internet Security. My name is Mark Rasch, and I am a Senior Vice President of Global Integrity Corporation, a wholly owned subsidiary of Science Applications International Corporation (SAIC) located in Reston, Virginia. Global Integrity works as an information security consulting company and resource for Fortune 100 companies, including online businesses, banks, brokerage houses, insurance companies, telecommunications and entertainment companies and other "dot com" industries. In this capacity, we test the overall computer security of our clients' sites, help them develop secure information architectures, and help them respond to attacks and incidents. We monitor and report to our clients about the most recent threats and vulnerabilities in cyberspace, and help them cooperate with regulators and law enforcement agencies where required or where appropriate.

Before joining Global Integrity, I was a trial attorney with the Fraud Section of the Criminal Division of the United States Department of Justice, principally responsible for investigating and prosecuting all computer and high technology crimes, including the prosecution of the Robert Morris Cornell Computer "Worm," and investigations of the Hannover Hackers of Clifford Stoll's "Cuckoo's Egg" fame, and investigations of Kevin Mitnick, the recently released computer hacker from California. When I left the Department of Justice in 1991, I was the sole attorney in the computer crime unit—and that was on a part-time basis. The Computer Crime and Intellectual Property Section of the Department of Justice today consists of more than a dozen attorneys and continues to grow.

As you requested, Chairman Gregg, I would like to address three principal topics today: the nature of the threats, vulnerabilities and trends in cyberspace and what the private sector is already doing about them; what, in my opinion, the government should and should not do to help protect the nation's critical infrastructure; and the adequacy of current law to combat cyber attacks on commercial systems.

As the Distributed Denial of Service attacks against Yahoo!, Amazon.com, e-Bay and e-Trade last week have made painfully clear, there are few rules in the electronic frontier, and information security has, for many, been the step-child of electronic commerce. For America to remain competitive—and to foster the growth of electronic commerce with its concomitant increases in productivity and convenience—protecting the critical electronic infrastructure is imperative.

The gravamen of the situation is essentially this. There are genuine threats to electronic commerce and to privacy and security of digital information, but none so significant that they should long deter or delay the growth of this wonderful technology. The same Internet that empowers a single individual to obtain a lower interest rate on a home mortgage by negotiating online empowers an individual hacker in a basement garage in Concord, New Hampshire to get information about a transaction in Charleston, South Carolina, or to shut down a dot com business in Palo

Alto, California. The Internet is no respecter of borders or of sovereignty. Government in general, and the U.S. government in particular, has a legitimate interest, and therefore a legitimate role, in encouraging the development of more secure, more robust, and more dependable computers and computer systems. However, government should not use the general insecurity about online commerce as an opportunity to take upon itself new powers of investigation, new powers to compel cooperation or reporting, or new opportunities to increase the regulatory burden on those doing e-business. The government can, though, do more to be a partner with the commercial sector and to promote trust and confidence in its abilities and its dedication to security.

No remarks of a lawyer would be complete without a disclaimer. Therefore, the Subcommittee should understand that while my remarks this morning represent the general views of Global Integrity and its parent, SAIC, as with any company of almost 40,000 employees, no single individual can truly represent all of the views of any collective entity. Moreover, while my views are colored by the work we have done with commercial enterprises—particularly in the financial services industry—I cannot and do not purport to speak for these entities. I don't think that they would be reticent about expressing their own views on this matter if asked.

The Sky is Falling?

The first question raised by the recent Distributed Denial of Service (dDOS) is whether this means that Chicken Little was right. Is the sky actually falling? The answer is, of course, maybe. The recent attacks have emphasized the inherent fragility of the public Internet that we have come to rely upon. The attacks themselves are not new, nor are the methods for perpetuating them. It is important to emphasize the fact that none of the "affected" websites—Yahoo!, e*Trade, e-Bay or CNN—were themselves "hacked." Nobody broke into these sites, nobody stole sensitive information from these sites, and nobody altered or damaged information resident on these sites. While there is some comfort to be found in these observations, the fact that a hacker or a few hackers, using a well known and fairly well publicized methodology, could nonetheless cripple these sites (albeit for a short period of time) demonstrates the interdependence of those on the web, and the vulnerability of all netizens to such attacks.

The Rise In CyberAttacks

According to Department of Justice statistics, cybercrime cases have increased 43 percent from 1977 to 1999. Reports and analyses conducted by the Computer Security Institute, the FBI, the Computer Emergency Response Team, SANS, as well as Global Integrity Corporation's data confirm the increase of computer related incidents and cyber attacks. By incorporating and synthesizing all available data from government studies, private industry surveys, research/academic research, information security reports, law enforcement statistics, public data and media reports and, most importantly, the live data, intelligence, and incidents worked by GLOBAL INTEGRITY, we have identified the following trends in cyber attacks:

—Distributed attacks are increasing, specifically indicated by the activity in late 1999 through the events of last week.

—Compromising the same vulnerabilities in systems is the predominant method of attack. Attackers are using the known and publicized security holes to compromise systems.

—Most incidents and penetrations seem to be attacks of opportunity.

—The release of point and click tools (complete programs, scripts and virus recipes) has made the ability to hack very easy and accessible to everyone. The numbers of attacks and door knocking have reflected this increase in accessibility and ability. The attacks can be perpetuated by so called "script kiddies" who can download these tools, or by more sophisticated hackers who can create or modify these tools to be more malicious or more difficult to detect.

—Generally speaking, attack coding is more sophisticated and some of it has been very creative.

—There has been an increasing number and sophistication of attacks against Microsoft systems; UNIX based attacks are remaining the same.

—Media exposure appears to be the catalyst for many attacks and appears to correlate to web attacks and hacks. Organizations appearing prominently in the news, launching new advertising campaigns, announcing IPO status, or holding press conferences seem to attract penetration attempts, hacks, and web defacement.

—Those attacks perpetrated by an insider seem to be driven by an internal change within the organization. Management changes, an acquisition or merger,

or a changed employment policy (i.e., benefits, retirement, stock options) seemed to be the catalyst (or at least one of the major precursors) to an attack.

Employees have also tended to take a more independent and individual view of their job and their work. Due to the emergence of the "dot.com" millionaires, the IPO frenzy, and the ease with which starting your own business was publicized in 1999, many employees are losing company loyalty. An upsurge in capitalism combined with the "American Dream," the ability to launch a new .com product quickly, obtain venture capital, the health of the stock market, and the ease and success of e-trading contribute to a foundational change in the American employee. The year 2000 will most likely bring even more changes in the workplace. Corporations should be particularly protective of their intellectual property.

Types of Attacks

In general, all types of attacks have increased to some degree during 1999. However, the greatest increases have been noted in theft of intellectual property, unauthorized insider access, insider abuse, and system penetration by an external party.

—Theft of Proprietary Information and Intellectual Property has increased 15 percent from 1998.
—Unauthorized Access by an Insider has increased 28 percent from 1998.
—Insider Abuse of Internet (i.e., e-trading, pornography, e-mail abuse) has increased 17 percent since 1998.
—System Penetration by External Parties has increased 32 percent from 1998.

Other types of attacks such as viruses and denial of service have been reported less in public and government surveys; however, these statistics may not reflect the true state of affairs. Global Integrity has observed both increases in virus-related attacks as well as denial of service attacks. Even though raw numbers may reflect a drop in actual reported incidents, the interpretation of these decreases are meaningful. Those corporations who have experienced a decrease in overall quantity of virus attacks may have also experienced an increase in the "quality" or system devastation of the fewer attacks. The viruses that have recently been observed are more sophisticated and complicated than viruses seen in the last two years.

In addition to the above mentioned attack types, we have seen as many as ten different attack types: Theft of intellectual property; sabotage to systems and networks; system penetration by an external party; insider abuse; financial fraud; denial of service; virus; unauthorized insider use of systems; web attacks and defacement; and other.

In addition to the attack types directly on corporate systems and networks described above, a secondary type of attack has been occurring. Employees and external personnel have caused damage to companies by their postings and communication on the Internet and World Wide Web. Either originating from inside their workplace or from home, human communication on-line has increased the vulnerability of corporate information assets. Global Integrity has assessed the on-line threat to include seven major categories:

—The disclosure of client related information;
—Overt threats to personnel or facilities;
—Disclosure of stock pricing and stock manipulation;
—The disclosure of technical information about corporate system and network architecture;
—Disclosure of intellectual property information and/or research and developments secrets;
—Trademark violations; and
—Other.

Global Integrity has also noted a trend in "jurisdictional jumping" where an attacker jumps or passes through several borders in order to appear to be originating the attack from a foreign country. Many of the 1999 overseas activities have also originated in countries and third world nations where on-line laws and guidelines are non-existent. Attacks originating from various foreign points appeared to increase. Another trend appears to include the behavior of a foreign national in U.S. based companies. Global Integrity has likewise detected a trend in foreign nationals, who are internal employees (or contractors) who have attacked the company from both a systems-network perspective, but also from inappropriate on-line communications.

Trends in Computer Attacks

The major new trends are perceived to include:

—More sophisticated attacks using both available and created tools, such as the "stacheldraht" distributed denial of service attack tool
—A greater prevalence of coordinated attacks from multiple sources

—Cross-cultural and cross-national origin of attacks
—Increased "disappearance" of intellectual property for personal benefit to spin off a new company or business as well as to sell to a competitor or other interested buyer
—An increase in attacks from out of the U.S., particularly from Eastern Europe
—An increase in the use of social engineering to acquire intellectual property, proprietary information, and sensitive information from commercial industries
—More encryption techniques will be used to hide files, network traffic, and other information
—An increase in attacks, due to the proliferation of on-line banking, which will lead to the compromise of personal and home systems. As the value of data on the home systems increase, so will the probability of attack. Those employees who work out of their homes on a personal or corporate system will become more vulnerable.
—An increase in coordinated and distributed DOS attacks
—A lowering of security standards and hiring standards, due to a shortage of IT professionals. Other security and HR standards such as criminal checks and background checks may be overlooked in order to hire quickly with the needed skill sets. If these vetting and screening procedures are not maintained, an increase in insider attacks will most likely occur.
—An increase in number and sophistication of self-mailing viruses as well as copycat or mutated viruses.

What the Private Sector Is Doing

It is difficult to generalize about the activities of a constituency as diverse as that of the Internet. Some institutions have taken information protection and security extremely seriously, and have dedicated significant energies and resources to protecting the information on the web. Other web-based enterprises deliberately act as a conduit for hackers or others to share information about propagating attacks. By necessity, the individuals and organizations Global Integrity deals with, for the most part, have at least taken the first steps. They have identified the need to prevent unauthorized and abusive uses of their computers and computer systems. Thus, our experiences are likely not representative of the Internet as a whole. Moreover, the bulk of our confidential client base—more than 70 percent—are in the financial services industry. These institutions, banks, brokerage houses, and insurance companies have long had a tradition and commitment to protecting confidentiality of information.

Information Sharing in the Private Sector

One of the concerns addressed in Presidential Decision Directive (PDD) 63 about the state of the critical infrastructure is the problem of information sharing in the private sector. This is of particular concern since the bulk of the nation's critical infrastructure—the computers and computer networks which make the nation run—are in the hands of the regulated private sector. The financial services, energy, transportation, and telecommunications industries are not owned by the government, but rather by the private sector. With deregulation and competition, information protection could be used as a competitive tool, allowing one company to keep secret tools for protecting itself, at the expense of the industry as a whole.

The FS/ISAC Model

In order to combat this problem, and to help promote an overall secure infrastructure, the financial services industry has been the first to create a formalized mechanism to share information about computer security threats, vulnerabilities and incidents between and among its members. The Financial Services Information Sharing and Analysis Center—FS/ISAC—formally launched on October 1, 1999, and hosted by Global Integrity, is a tool which permits its members to anonymously share information which could help protect the industry as a whole. Fears of publicity, fears of inviting additional attacks, fears of confidentiality, and fears of anti-trust liabilities have, in the past, limited the willingness of industry members to share information. Nobody wants it to be reported in the front page of "The Washington Post" that a bank or financial institution has been the victim of an attack or an attempted attack. The FS/ISAC provides a means for sharing information—and for distributing threat information obtained from government sources—without fear of attribution or publicity. Nothing contained in the FS/ISAC rules or regulations alters the obligations of banks or other financial institutions to report criminal activities to regulators or law enforcement agencies. Nothing contained in the ISAC regulations precludes or discourages reporting of incidents, except that information learned exclusively from the information provided in the ISAC database remains confidential unless disclosed by the source of that information.

The FS/ISAC represents a form of public-private cooperation that can be a model for the future. The Treasury Department and the SEC support but do not run the FS/ISAC. It is a separate entity with its own governing board made up of representatives of various financial institutions. The government may use the FS/ISAC as a means for disseminating information TO members of the financial services industry, but relies on traditional reporting requirements for obtaining information from the industry. It works to facilitate inter-corporate information sharing to help protect one of the critical infrastructures.

Information Sharing and Public Dissemination

It was reported yesterday by Ted Bridis of the Associated Press that "computer experts at some of the nation's largest financial institutions received detailed warnings of impending threats and that banking officials never passed their detailed warnings to the FBI or other law enforcement agencies, even as alerts escalated last week from the first assault against the Yahoo! Web site on to eBay, Amazon, Buy.Com, CNN and others." The report continued by observing that "Participating banks weren't allowed to share the warnings with government investigators under rules of an unusual $1.5 million private security network created in recent months for the financial industry." This report is based upon a series of unrelated events and is not entirely correct.

In mid August 1999, a distributed denial of service attack was launched against a Midwestern university. This attack was discussed in a mailing list discussion on the Forum of Incident Response Teams (FIRST) and was available to information security professionals who were members of FIRST and who had subscribed to the list. Utilizing this and other information gathered by Global Integrity, on September 9, 1999 Global Integrity sent an advisory to subscribers to its Rapid Emergency Action Crisis Team (REACT) Advisory Service. This service is a fee-based subscription service that distributes advisories about a myriad of computer security incidents, vulnerabilities and threats. The issuance of this advisory by Global Integrity predated by almost a month the formal initiation of the FS/ISAC.

On October 21, 1999, a similar analysis was publicly issued by Dave Dittrich, who wrote an analysis of the Trinoo attack tool. A copy of this posting can be found on the web at http://staff.washington.edu/dittrich/misc/trinoo.analysis.

On November 2, 1999 the Computer Emergency Response Team at Carnegie Mellon University held a conference, open to the public, in which the dDOS attack scenarios were discussed, and a paper describing how companies should respond to such dDOS attacks was published on the CERT website at www.cert.org. A more detailed advisory was issued by CERT on November 18, 1999, and Global Integrity issued a more detailed advisory to the REACT subscribers the following day. A similar advisory was posted for members of the newly formed FS/ISAC.

On December 6, 1999, the National Infrastructure Protection Commission (NIPC) issued advisory 99–029 describing the denial of service attacks and the manner in which they could be used to attack computer systems. The NIPC advisory specifically described the TRINOO, and Tribe Flood Network (or TFN & tfn2k) attacks on January 19, 2000, and advised that:

> * * * the NIPC has seen multiple reports of intruders installing distributed denial of service tools on various computer systems, to create large networks of hosts capable of launching significant coordinated packet flooding denial of service attacks. Installation has been accomplished primarily through compromises exploiting known sun rpc vulnerabilities. These multiple denial of service tools include TRINOO, and Tribe Flood Network (or TFN & tfn2k), and have been reported on many systems. The NIPC is highly concerned about the scale and significance of these reports, for the following reasons:
>
> —Many of the victims have high bandwidth Internet connections, representing a possibly significant threat to Internet traffic.
>
> —The technical vulnerabilities used to install these denial of service tools are widespread, well known and readily accessible on most networked systems throughout the Internet.
>
> —The tools appear to be undergoing active development, testing and deployment on the Internet.
>
> —The activity often stops once system owners start filtering for TRINOO/TFN and related activity.

On December 28, 1999 the Computer Emergency Response Team at Carnegie Mellon issued another advisory further describing the dDOS tools and their effects. At about this time, Global Integrity began to receive reports from clients that versions of these attacks were actually being launched—albeit on a limited scale. These con-

sisted of reports of coordinated scans of systems and Trojan horse attacks on systems—indicia of automated efforts that might have been attempts to insert software "agents" on computers on the net. Such attacks are not uncommon, and represented yet another attempt to exploit widely know vulnerabilities in computer systems. On December 28, 1999, Global Integrity issued advisories to its customers about both the methodology of the dDOS attacks and the fact that such scans were ongoing.

On December 30, 1999, the NIPC again issued an advisory to the public warning about the Trinoo/TFN/TFN2k toolkits, and the way they could be used to perpetuate a denial of service attack. This was followed on January 3, 2000 by an advisory issued by CERT detailing new developments in the denial of service software. On January 6, 2000 Global Integrity advised its clients, including subscribers to the FS/ISAC, that it had seen increased dDOS attack activity, including continued efforts to probe insecure systems on the Internet.

On February 8, 2000, Global Integrity issued a press release, which had been prepared earlier, again describing the nature of these vulnerabilities, and advising potential victims of such attacks of Global Integrity's ability to assist in responding or tracing such attacks. This release was, like the earlier NIPC, CERT and other advisories, widely disseminated. The news release was not prompted by any specific threat or incident, and indeed, was scheduled to be released some weeks earlier. Never underestimating the power of coincidence, within 12 hours of the issuance of the press release, the attacks against Yahoo! began. However, the FBI and the NIPC had long been aware of, and had long reported publicly about, the nature of these kinds of dDOS attacks.

When the dDOS attacks began, members of the FS/ISAC used the facilities and protocols previously established to share information about the attacks on an ongoing basis, and to coordinate an industry wide response. The nature of this particular attack required a detailed sharing of log and system information to effectively coordinate a response. Thus, rather than "hiding the ball" from both law enforcement and the public, the FS/ISAC and Global Integrity, like the NIPC, and CERT, attempted to widely disseminate information about the vulnerability before it was widely exploited. There were, to the best of my knowledge, no urgent e-mails or pages to FS/ISAC members prior to the attack—and during the attack, none were necessary. By then, the entire world knew of the attacks. However, when there are actual information security emergencies, the FS/ISAC will page its members and alert them to log on to the service to see the latest releases. In this way, FS/ISAC acts as a clearing house and early warning system, but it is only as good as the information it receives, and depends upon the continued vigilance and cooperation of its members.

Expansion of the FS/ISAC Information Sharing Model

It is contemplated that the FS/ISAC model can be and will be utilized as a template for voluntary industry cooperation and information sharing in other industries. Only through voluntary cooperation can this model work. A similar vehicle for voluntary cooperation has existed in the telecommunications industry for many years. This entity, known as NSTAC—the National Secure Telecommunications Advisory Commission—which includes in its members, Science Applications International Corporation, Global Integrity's parent company, facilitates voluntary information sharing in the telecommunications industry. Mandatory reporting to government agencies of security incidents or vulnerabilities will prove counter productive, as some will choose to report every "ping" or bad password use, and some will report only the most serious attacks or vulnerabilities.

What Role for Law Enforcement?

Protecting the information superhighway is not exclusively a law enforcement function any more than protecting the nation's highway system is the sole province of law enforcement. Ensuring that the highway is designed and implemented properly, that roadblocks and potholes are appropriately marked and repaired, that vehicles traveling are tested and safe is the province of standard setters, industry groups, and regulators. In many ways, the information superhighway is the same. The government can and should help set standards for secure infrastructures. The government can and should encourage the use of security technologies—including encryption technologies. The government can and should work with the private sector to ensure interoperability and emergency response capabilities. However, if these standards are perceived to come from the nation's law enforcement or intelligence communities, they will be met with distrust by both civil liberties groups and the commercial sector. The commercial sector—rightly or wrongly—perceives any encryption standards "approved" by the NSA as being inherently weakened.

This problem is emphasized in the area of incident response. By and large, commercial enterprises want to do the right thing, and want to work with law enforcement agencies to timely report and coordinate responses to information security incidents. Where incidents represent an immediate threat to public health or safety, there should be no question about reporting of such incidents, and generally there is none. The FBI, Secret Service, Department of Justice and other agencies have made great strides toward promoting public-private cooperation, addressing private sector security groups, conferences and public events, as well as working behind the scenes to foster greater confidence in law enforcement. In many cases individuals within corporate America responsible for security are themselves former law-enforcement officials, and the cooperation proceeds on an informal basis.

Despite these efforts, however, there is a problem of communication between the private sector and law enforcement. While both groups are committed to securing the web in general, they use different means and techniques. A successful case to law enforcement is when a public attack on a site results in the swift apprehension of a non-juvenile defendant, the speedy and public prosecution of the subject, culminating in a conviction and a sentence sufficient to act as both a specific and general deterrent.

To the private sector, such a result may be disastrous. The public nature of the trial would reveal the vulnerabilities in information security that were exploited. Public confidence in the security of the e-commerce site would be eroded, even if the site had done all that was feasible to prevent or deter the attack, and even if the company responded quickly and appropriately. Moreover, by calling in law enforcement, the company quickly loses control over the scope and pace of the investigation, its direction and whether or not it will become public. Law enforcement agencies are today much more sensitive to the concerns of the "victims" of these attacks. They are directed to conduct investigations in the manner that will be the least intrusive on the business operations of the company. Nevertheless, some disruption is inevitable. The "evidence" of the crime may be the web server that is essential to the ongoing business operation. Law enforcement may wish the attack to continue so that the suspect can be traced and apprehended, but the "victim" may simply want the attack to stop. It may turn out that the offender lies within the company that reported the offense, and that the company itself now faces the prospect of civil or criminal liability. All of these factors point to an inherent mistrust—for reasons real and imagined—of vesting in a law enforcement agency the sole or exclusive responsibility for critical infrastructure protection.

Nevertheless, as with highway traffic safety, law enforcement has and will continue to have a significant role in doing what it is trained to do: enforce the law. This response need not be solely reactive. Gathering and disseminating threat data may be an appropriate role of law enforcement. Whatever agency or department—or agencies or departments—that ultimately have the responsibility for infrastructure protection must have the confidence and participation of the commercial sector, and of the community at large to be effective.

Additional problems plague law enforcement agencies. It is difficult if not impossible for them to train and retain staff skilled in the subtleties and nuances of the new high technology crime scene. The pace of technological change coupled with the lure of the private sector may discourage all but the most dedicated staff from staying with law enforcement.

Law enforcement also is used to dealing with other law enforcement agencies in coordinating criminal responses. In the new Internet era, however, the primary investigators are no longer those with badges and guns. Computer crimes are detected and investigated initially by 23 year old overworked system administrators under the rubrick of "other duties as assigned." For those companies that have a computer incident response plan—fewer that 2 percent of the companies we surveyed—the next to be notified are the information security officers, legal staff, human resource and other security staffs. Only after this chain has been called into place are law enforcement likely to be notified. By then, the hacker may be long gone or the trail cold. The private sector lacks the authority to compel the cooperation of distant ISPs, and law enforcement lacks the information and training to protect a corporate infrastructure.

Add to these problems the fast pace of change of both the law and technology, the differences in rights to privacy in various countries, the inability of any individual law enforcement agency to act beyond its borders and the trans-national nature of computer crime, and we are left with serious impediments to relying upon law enforcement as a means of prevention of computer crime. We need better locks on computers, not better locks on jails to prevent this conduct.

Role of the Government

There are certain roles and functions that are and can be the province of the government. These include setting minimum standards for security and interoperability, conducting and supporting fundamental research on new security technologies—particularly in the area of biometrics and smart card technologies—promoting awareness of issues relating to information protection, ensuring greater international cooperation between law enforcement and other agencies, and bringing down barriers that inhibit such cooperation.

Setting of Standards

The government can and should set standards in cooperation with both Internet companies like Cisco, IBM and others, and telecommunications and software companies for security. These standards should both afford a reasonable degree of security and be attainable in a cost effective manner. Such standards should empower users to secure themselves, but should not be used as a "command and control" mechanism to force new regulatory burdens on users. In essence, the goal should be to standardize for interoperability and security, and not to mandate a particular technology.

Research and Development

Computers and computer networks are inherently complicated. Moreover, it is always easier to tear down a building than it is to design and build it. The government has a legitimate role in funding and supporting basic and applied research in the area of information security. Let us not forget that the Internet itself was the outgrowth of basic research initiatives by the Department of Defense Advance Research Projects Agency. Such research funding should be across disciplines—not limited to computer sciences. Security depends not only on hardware and software, but also on policies, practices, and personnel. We need not only to understand the vulnerabilities of the infrastructure, but to understand who exploits them and why.

Education and Training

Education and training is an essential component of information protection. No passwords, or poor passwords, are the most common and cost efficient way to obtain unauthorized access to a computer or computer system. Users, administrators and others must be educated about the appropriate use and threats to computer systems. The bulk of this training should be done by companies educating their employees about the need to be vigilant, and the government educating its employees and contractors about the need for security precautions.

In addition to user education, the government has a role in promoting the development of undergraduate and graduate level programs in information security. Global Integrity has established a mentoring program in this area with several universities, including Purdue University, and I have taught classes in information security at the George Washington University and a distance learning program at James Madison University. The dearth of trained professionals, inside and outside of government, may cause the private sector to unfortunately reach out—from sheer desperation or a misguided trust—to untrained individuals at best, or computer hackers themselves. Basic levels of competence, possibly including independent non governmental certification programs, will assist in ensuring that there is a cadre of trained information security professionals.

Technical Support

Many information security attacks are beyond the technical capabilities of any individual company, and no individual company should be required to bear the burden of fixing what are essentially societal problems. The government, in cooperation with private industry, can provide meaningful databases and technical support to assist.

Promoting New Security Technologies

A lesson should be learned from the recent debates over encryption. After almost ten years of debate, the government has finally liberalized the regulations concerning the use and export of commercial encryption software to the point where most companies now feel free to create and use such software to protect confidentiality, integrity and availability of information. However, the efforts to restrict the export of such software—while motivated by a legitimate desire to protect national security and promote the ability of law enforcement and intelligence agencies to lawfully intercept communications—proved to be counterproductive, and had the unfortunate effect of making individual communications less secure. At present, the default for most companies and government agencies is to send electronic commu-

nications in an unencrypted and therefore insecure manner. For true information protection, the default should be seamless effective encryption.

Protecting the Government's Own Infrastructure

The government should also spend the resources necessary to protect and defend its own infrastructure—civilian and military. Most of the current Administration's efforts reflected in its budget requests are geared toward this goal. For example, on February 15, 2000 the White House issued a press release indicating a proposal, reflected in the budget previously submitted for a 15 percent increase in the fiscal year 2000 request for spending on critical infrastructure to reflect a total budge for such operations of $2 billion. The Administration proposes spending $606 million for research and development. These expenditures are geared principally toward protecting the government's infrastructure, training those charged with protecting government systems, and establishing an early warning system to detect attempted penetration into the government's own computers.

What the Government should not do

The government should not seize the publicity surrounding these incidents to take upon itself new powers of regulation or impose new burdens upon those operating on the web. Any such regulations would likely be ineffective, counter productive, and would impose a disproportionate compliance burden on U.S. companies.

The government must respect the fundamental rights of privacy—including a respect for the right of anonymity where appropriate. For political and social discourse to flourish on the web—in America and abroad—governments must agree not to unduly burden the privacy rights of the electronic community.

The government should not use the legitimate threats to computer systems as a justification for increased monitoring or surveillance of its citizens or others. While much of the traffic on the Internet is "public" in the sense that the IP traffic is transmitted over insecure routers and servers, the government should not create a database of "normal" traffic patterns or surveil otherwise innocent Internet traffic.

Most importantly, the government should not rush to pass new laws or new regulations unless and until it is demonstrated that current legal regimes are both inadequate to solve the problems, and are not preserving other fundamental rights or liberties. We should not sacrifice liberty at the altar of security.

Legal Issues

One question raised by the recent attacks is whether the current legal regime is sufficient to respond. Let me begin by observing that the intentional transmission of a computer program with the intent to disrupt or deny the lawful use of a computer system is already an offense under 18 U.S.C. 1030, as well as a host of state criminal statutes. Many in the media have speculated whether the current penalties—up to five years incarceration (per incident) and a fine of either $250,000 or the amount of loss or gain resulting from the offense (together with possible forfeiture of proceeds or instrumentalities of the offense)—is sufficient to deter such conduct. This is especially a concern where the offenders may be—and I stress may be—juveniles for whom such punishments may not even be available.

At the outset, I observe that the chances of detection and prosecution of computer hackers is very small. A handful of high profile cases have been reported. These include:

—Prosecution of Andrew Miffleton a/k/a Daphtpunk in December of 1999 in Dallas, Texas for trafficking in root access codes which would permit a user to break into and take over a computer system.

—The December 1999 prosecution of David Smith in the District of New Jersey for creating and releasing the so-called Melissa virus which reportedly caused more than $80 million in damage.

—The November 1999 prosecution of Jeffrey Gerard Levy in Eugene, Oregon for the criminal posting to the Internet of pirated software valued at at least $70,000. Levy was sentenced to probation.

—The November 1999 prosecution in the Eastern District of Virginia of 19 year old Eric Burns, a/k/a ZYKLON, for hacking into and altering the web pages of the USIA, NATO, and the Vice-President, as well as commercial sites in the Northern Virginia area.

—The multiple prosecutions of Kevin Mitnick, released earlier this year for a series of computer attacks and cell phone clones.

—The prosecution, in Brooklyn, New York in March 1998, of Eugene Kashpureff for invading the Internet Domain Name System (DNS) and rerouting internet traffic intended to go to Global Integrity sister company Network Solutions to his own website.

—The international cooperation which resulted in the Israeli arrest of Ehud Tenebaum, a hacker who broke into hundreds of insecure U.S. government sites. Tenebaum is now reportedly working as a computer security consultant.

In none of these cases would additional punishments necessarily have served to prevent or deter the criminal activity. Because hacking offenses generally can result in multiple counts of conviction, the five year statutory cap on punishment is somewhat illusory. The true punishment for computer hackers is dictated not by the provisions of the United States Code, but rather by the provisions of the United States Sentencing Guidelines, which treat computer hacking in a manner identical to the outright "theft" of money.

A convicted hacker is sentenced under U.S.S.G. 2F1.1, which attempts to measure either the "gain" or "loss" resulting from the criminal activity. The loss may include things like lost business opportunities resulting from downtime, or the cost of repair or replacement, but is ill defined. Moreover, such an analysis may overstate the seriousness of an offense like that of the Melissa virus. While the virus itself caused massive disruption and inconvenience, and is deserving of stringent punishment for deterrence, one can reasonably question whether the defendant should be sentenced on the same par as someone who literally "stole" $80 million. The guidelines likewise serve to understate the seriousness of hacker offenses. Invasions of privacy, the inconvenience associated with having to obtain new credit card numbers or a new identity, the loss of confidence or business opportunities and other collateral losses are not adequately captured in the manner in which we punish or attempt to punish hackers.

Conclusion

Undoubtedly, there will be call for new laws regarding search and seizure powers, calling for the streamlining of procedures to permit multi districts investigations and international investigations, and possibly calling for additional powers of investigation. I urge the Subcommittee to tread lightly. Some of these may be warranted and some may not. The application of old rules to new technologies results in many absurdities. The government should encourage the use of new technologies by recognizing the binding nature of digital or electronic signatures, and promote the use of the Internet. The government should not use the new medium of cyberspace to inflict draconian regulations, assume new authority, or take upon itself the mantle of the protector or defender of cyberspace. The obligation and responsibility for protection of private data lies in a cooperative public-private partnership.

I thank the Subcommittee for the opportunity to present my views and welcome any questions members might have.

Senator GREGG. I think most of you answered most of my questions because you pretty well summarized your view as to the role of the government relative to e-commerce. You heard the Attorney General say that she felt that there was a comfort level being developed, and you heard the Director of FBI say the same thing. I would be interested in whether you folks feel there is a comfort level that is being developed?

Mr. RICHARDS. Senator, if I can, the Internet Alliance's Law Enforcement Security Council was formed last fall for just this reason, partly because we need the daily dialogue, and we need to do it in a group sense as well as an individual company sense for many of the reasons that were talked about here. I think the curve is exactly in the right direction, lots of talk, lots of specifics. What this has to get down to is a level of trust but also concrete accomplishments. Training is a critical area. We could talk about training all day. It is the steps we will take together that ought to be a bellwether for you.

Senator GREGG. Anybody else have thoughts on this?

Mr. CHESNUT. With eBay we agree. We believe that the level of cooperation has been growing, certainly over the last year, and there has been a good fundamental level of trust that has been established I know at eBay between eBay and law enforcement. So we are very happy in that area.

Mr. RASCH. I find that trust is based on personal relationships. Rather than having an agency or a company call the FBI, it is much easier if someone in the company is calling a friend of theirs at the FBI. We have started to do that and establish personal relationships between these electronic companies and law enforcement agencies. I think we can do a lot more.

Senator GREGG. How do you handle the fact that a lot of this happens from out of the country? I mean as the FBI Director said, their investigation is leading them to Germany, it appears, and we have other reports in the press that there may be other countries where these originated from.

Mr. RICHARDS. Senator, the Internet Alliance and others here work with, and our own DOJ and FBI work with, Interpol and others. First I just have to tell you from my own direct experience, you know, our best folks at FBI and DOJ are extremely well thought of by their peers around the world. I just want to make clear that there is a high level of regard for our technical and strategic expertise. That is why we need to add some more resources to that. But the issues are real, and frankly, international law enforcement is not moving at Internet time. I think we are working hard here to get our relationships moving on Internet time, you know, very, very quickly, but we see lots of bureaucracy when we leave North America. So we are really concerned about that.

The fundamentals may not end up being elaborate treaties or protocols. They may end up being in 90 percent of the cases really good cooperation using standard techniques but applied to the Internet through the rule of law. And that is what we need to focus on next.

Mr. CHESNUT. The international aspects certainly present some different challenges. For a company like eBay, we actually have sites with employees in different countries, such as Germany and Australia and the United Kingdom, but when I spoke earlier about establishing a partnership with law enforcement, we view that partnership to be with law enforcement in different countries and to reach out and to make contact and explain what we are about and at least establish a protocol so that if something happens we can find each other and provide information under appropriate circumstances. eBay has been doing that as well. We also work through the FBI because, again, they have a presence in many countries overseas, and while it poses challenges, it is not anything that is insurmountable.

Senator GREGG. Mr. Rasch, you said or were quoted as saying that the absolute worst people to coordinate law enforcement would be the FBI. Maybe give me—if that is an accurate quote, give me your reasons.

Mr. RASCH. The absolutely worst people to coordinate security is law enforcement, and not the FBI in particular, but the worst people to coordinate security is law enforcement. Law enforcements were always to enforce the law and to investigate and prosecute criminal activity. Just as I would not feel comfortable necessarily in having law enforcement come in and install my security system. There is a fundamental mistrust here. And there is a difference between protecting cyberspace and developing secure architectures, which is a role for agencies like the Commerce Department, like

NIST, and the fundamental research and enforcing and investigating criminal activities which is the role of the FBI, the Secret Service, and the other law enforcement agencies. We should not allow the law enforcement agencies to take upon themselves the responsibility for protecting critical infrastructure or designing architectures because they will not have necessarily the confidence of the private sector.

If I am buying a product, a security product, with an FBI seal of approval, I am going to have a fundamental mistrust of that or more importantly the NSA [National Security Agency]. There is a fundamental mistrust there because there is a belief, whether it is rational or not, that that product has been maximized to allow FBI or NSA to engage in its other functions. For example, surveillance.

Senator GREGG. That was an excellent point. You all talked, certainly Mr. Richards and Mr. Chesnut talked, at length about the need for more resources in this area. I will simply tell you that as far as this committee is concerned—and we are in charge of resources, by the way—we will be putting more resources in this area. Our concern is that it be coordinated, that it be used effectively, and we do not end up going down the wrong path—that we do not end up creating a three-headed horse in response to the issue.

So industry's role here is critical, and I appreciate your taking the time to come today. I appreciate your input, and I hope that you will, and I know you will, continue to aggressively pursue the interaction between the functions of law enforcement and the functions of research within the government and private sector. Do you folks have anything else you wish to add? Well, thank you very much. I appreciate your time.

CONCLUSION OF HEARING

I would note that the subcommittee will be holding a hearing on February 24 with Commerce Secretary Daley. We are also going to continue the issue of the Internet, specifically at the request of Senator Hollings. I strongly support his interest in this area, dealing with the SEC and the FTC and the issue of fraud on the Internet, which also happens to come under the jurisdiction of this committee. So we may change our title to the "Internet Appropriations Committee." But in any event we are going to be pursuing this issue in other forums, in other areas. Thank you very much.

[Whereupon, at 12:25 p.m., Wednesday, February 16, the hearing was concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]

○

Document No. 46