S. HRG. 106–839

CYBER ATTACKS: REMOVING ROADBLOCKS TO INVESTIGATION AND INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

EXAMINING THE INCIDENCE OF CYBER ATTACKS ON THE NATION'S INFORMATION SYSTEMS, FOCUSING ON REMOVING ROADBLOCKS TO INVESTIGATION AND INFORMATION SHARING

MARCH 28, 2000

Serial No. J–106–72

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

69–358 CC WASHINGTON : 2001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

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

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

JON KYL, Arizona, *Chairman*

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

STEPHEN HIGGINS, *Chief Counsel*
NEIL QUINTER, *Minority Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

APPENDIX

QUESTIONS AND ANSWERS

CYBER ATTACKS: REMOVING ROADBLOCKS TO INVESTIGATION AND INFORMATION SHARING

TUESDAY, MARCH 28, 2000

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

The subcommittee met, pursuant to notice, at 10:03 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl (chairman of the subcommittee) presiding.

Also present: Senators Grassley, Feinstein, Schumer, and Bennett [ex officio.]

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

Senator KYL. The subcommittee will please come to order. Let me first welcome everyone to this hearing of the Subcommittee on Technology, Terrorism, and Government Information.

Today, we will examine various roadblocks to the protection of our information systems from cyber attack. Using the recent denial of service attacks as a backdrop, we will discuss some of the things that inhibit swift investigation and prosecution of cyber crimes, and the sharing of vulnerability and threat information among the private sector and with organizations affiliated with the Federal Government.

This is the sixth public hearing we have held in the past 3 years on the critical issue of securing our Nation's information infrastructure. The issue is now beginning to receive national attention.

The latest attacks on eight well-known Internet sites like eBay, Yahoo and CNN raised public awareness and hopefully will serve as a wakeup call about the need to protect our critical computer networks. Uncertainty caused by the attacks contributed to a 258-point drop in the Dow Jones Industrial Average and halted a string of 3 days of consecutive record-high closes of the technology-laden Nasdaq Composite Index.

As the New York Times noted in an editorial, "Just when Americans have begun to get accustomed to the pervasive influence of the Internet, a wave of anonymous assaults on Web sites has roiled the stability of the newly emerging cyber world." What the Times didn't say was that although disruption to these sites was substan-

tial, the damage did not even approach what it could have been, based on the Internet's known vulnerabilities.

Catching and punishing those who commit cyber crimes is essential for deterring future attacks. When a cyber attack occurs, it is not initially apparent whether the perpetrator is a mischievous teenager, a professional hacker, a terrorist group, or even a hostile nation. Law enforcement must be equipped with the resources and the authorities necessary to swiftly trace a cyber attack back to its source and appropriately prosecute.

Today, we will discuss some impediments to law enforcement in cyber space and how the bill that I recently introduced with Senator Schumer would remove some of these impediments. In particular, the bill would modify the trap and trace authority so that law enforcement will no longer need to obtain a warrant in every jurisdiction through which a cyber attack traveled. It will also remove the current $5,000 minimum in damages for a case to be considered for Federal prosecution, and it will remove the current 6-month minimum sentence for cyber crimes that frankly has led to lesser serious attacks not being prosecuted, and finally allows youths 15 or older to be considered for Federal prosecution for committing serious computer crimes.

The recent attacks also illustrated one crucial point that must be understood when dealing with securing the information infrastructure. We are only as strong as our weakest link. If only one sector of society heeds warnings and fixes computer vulnerabilities, that is not enough. The cyber criminal, terrorist, or enemy nation will search for another sector that has ignored warnings and not used proper computer security.

The February denial of service attackers first infected university computers with programs and then launched massive amounts of invalid inquiries to the victims, shutting them down. Computer capacity is increasing so rapidly that individuals with personal computers at home and work can now be used for similar types of attacks. We must examine the best way to secure all parts of our information infrastructure from attack. In order to do that, all individuals, businesses, and agencies with computer must get serious about security.

Last fall, Carnegie Mellon University's Computer Emergency Response Team posted warnings about these types of denial of service attacks. The FBI's National Infrastructure Protection Center, NIPC, also posted warnings and even provided a tool for anyone to download to check to see if their system was infected with the attack program. Many people heeded those warnings and used the tool, but not enough to prevent the attacks from occurring. We need to encourage and perhaps even consider some kind of mandate to individuals and systems administrators to tap into the resources available to ensure their own security and that of others connected to the Internet.

Finally, overall protection from attack necessitates that information about cyber vulnerabilities, threats and attacks be communicated among companies and with government agencies. Cooperation among competitors, while adhering to underlying antitrust laws, is necessary to create information sharing and analysis centers in each portion of the private sector. Additionally, the Freedom

of Information Act may need to be updated to encourage companies to share information with the Federal Government. Communication is crucial for protection and these roadblocks must be removed.

Our witnesses today are well suited to address these issues. Director Louis Freeh of the FBI will discuss limitations to effective investigation and prosecution of cyber crimes under current law. He will explain how the Schumer–Kyl bill brings some provisions of current law into the computer age.

On our second panel, Mr. Rich Pethia, Director of the Computer Emergency Response Team at the Carnegie Mellon University, will testify about CERT's role in analysis of computer vulnerabilities and better ways of getting the word out and ensuring that warnings are heeded.

Mr. Harris Miller, president of the Information Technology Association of America, will present industry's perspective on impediments to information sharing of threats and vulnerabilities among private sector companies and government agencies.

Before we hear from the witnesses, I would now like to turn to Senator Feinstein for any opening remarks that she would like to make.

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

Senator FEINSTEIN. Thank you very much, Mr. Chairman, and thanks for holding these hearings.

Welcome, Director Freeh, it is good to see you again.

The recent distributed denial of service attacks on Yahoo, eBay, E*Trade, CNN and Amazon, I think, have brought home how vulnerable the Internet is to electronic sabotage. Indeed, as our first witness well knows, even the FBI's own website was brought down last month by denial of service attack.

These attacks have not only disrupted electronic commerce, but have also had a debilitating effect on public confidence in the Internet. A recent poll by PC Data Online, for example, showed that the attacks caused 37 percent of Internet users to change their mind about the vulnerability of the Internet. Moreover, over half of these users said that attacks had caused them to alter their online behavior, with more than 80 percent saying that they would be less likely to shop over the Internet in the future.

These attacks really shouldn't have been a surprise to anyone. Long before the attacks occurred last February, the FBI, the National Institute of Standards and Technology, and Carnegie Mellon's Emergency Response Team Center had all issued alerts and even provided filtering or detection tools to help prevent the attacks. Unfortunately, however, many companies have not received these alerts or have ignored them.

We may not be able to prevent denial of service attacks completely, but we must explore ways to encourage industry and government to share information to prevent such attacks. We must also look into means of removing obstacles to investigate and prosecute perpetrators of these attacks.

I hope the hearings this subcommittee has been having will help us better understand the nature of cyber attacks and suggest possible legislative or private sector solutions to remove these obsta-

cles, and also to suggest deterrent actions and comment on whether our penalty structure is, in fact, adequate. I also hope that the hearings will raise the profile of the problem of cyber attacks, encouraging people to take precautions to prevent their computers from being hijacked or part of a DDOS attack, and if they run a website, to look into filtering or detection technology to stop DDOS attacks when they occur.

So thanks very much, Mr. Chairman, and I look forward to working with you on this issue.

Senator KYL. Thank you, Senator Feinstein.

Senator Grassley, do you have any opening remarks?

Senator GRASSLEY. No.

Senator KYL. Senator Schumer, incidentally I am not sure you were here when I referred to the Schumer-Kyl bill, a strange phenomenon in Washington.

Senator FEINSTEIN. In that order, too.

Senator KYL. But I did that in recognition of your leadership in helping to put it together.

STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Well, I thank you, Mr. Chairman, and I was going to thank you for that generosity. In fact, we were in a meeting on the asset forfeiture bill and Henry Hyde, when I walked into the room, said—when I was subcommittee chairman, he came up to me and said there was a great idea about dealing with children who were transported across State lines. And Hyde said to me, well, you carry the bill and I will cosponsor it and we will move it, because that is how things were done in the House. And I said to Henry, why don't you carry it and I will cosponsor it? And he said when he became chairman, that is why he always treated me so well on the committee.

So I thank you. It is returning of a good deed, and I know you wouldn't wish this, Mr. Chairman, but if I ever become chairman of this subcommittee, I will repay the favor many times over. I also want to thank you for your leadership on this subcommittee and in so many different areas where we do work together, particularly in areas like this involving crime and terrorism and things like that.

I also want to thank Director Freeh for being here, as well as our other witnesses, and would ask that my entire statement be put in the record.

We all know, as Senator Feinstein mentioned, last month's denial of service attacks on companies like Amazon.com and ZDNet underscore the new threats to our security and our economy that are posed by online crime in an increasingly networked society. These DOS attacks show how easy it is to break into the country's most prized computer networks and how hamstrung law enforcement can be in apprehending them.

To me, the problem is threefold. First, most computer systems are not secure, and security was a relatively low priority in the development of computer software and Internet systems. I hope and believe that is changing.

Second, hacking is sometimes still considered more of a prank than a crime, even though hacking can cost billions of dollars to the economy.

And, third, our laws, even our computer laws, are set up for a world that travels at subsonic speed, while hacking crimes move at the speed of light.

Now, we can't solve all of these problems through legislation or government action. The private sector has to take the lead, and while government can provide some help with research and a market for secure systems by purchasing only hackproof computers and software, we all know that private companies have to take the lead in making systems more secure.

What Senator Kyl and I are trying to do here is make it possible for law enforcement to catch hackers in the act by modernizing our laws, making the crime of hacking a more serious offense befitting the serious damage that it can cause.

I have also become convinced that many of the best solutions are far-reaching and require, among other things, significant cooperation from foreign governments. We shouldn't fool ourselves into thinking Congress alone can solve this problem even from a law enforcement perspective and that we can do it right away.

So last month Senator Kyl and I introduced the Schumer-Kyl, for which I thank you again, high-tech crime bill, S. 2092, that for the first time provides law enforcement with nationwide trap and trace authority. As you know, Mr. Chairman, under current law investigators who are trying to track a hacker must obtain a trap and trace order in each jurisdiction through which an electronic communication is made.

For example, to trace an online communication between two cyber terrorists that starts at a computer in New York, goes through a server in New Jersey, bounces off a computer in Wisconsin, and then ends up in San Francisco, under current law investigators are forced to go to court in each jurisdiction permitting the trace. And if one court slows them down, they are way behind the eight ball.

What our bill does is amend current law to authorize the issuance of a single order to completely trace online communications to its source, regardless of how many intermediary sites it passes through. Law enforcement still must meet the same burden to obtain such an order. The only difference is they don't have to repeat the process over and over again.

Our bill, as you may have mentioned, Mr. Chairman, also makes several other changes. One deficiency of the present law is its requirement of proof of damages in excess of $5,000. In several cases, prosecutors have found that while computer intruders had attempted to harm computers vital to our critical infrastructure, it was very difficult to prove the $5,000 in damages. Our legislation unambiguously permits Federal jurisdiction at the outset of an unauthorized intrusion into critical infrastructure systems rather than having investigations wait for any damage assessment. Crimes that exceed $5,000 will be prosecuted as felonies, and crimes below that amount will be defined as misdemeanors. Those are the two main provisions of the bill.

Just finally, Mr. Chairman, I would like to note and add to the record a letter received from the Fraternal Order of Police supporting our bill, which described these provisions as important changes to existing law which will empower law enforcement to deal appropriately with the new computer criminal.

Mr. Chairman, in conclusion, the creation of a more secure environment in cyberspace is good for everyone but criminals. The denial of service attacks have boosted the prominence of the issue, but the real key will be whether we can come up with appropriate solutions that will deter and punish crime without impinging on the rights of individuals and without slowing down the booming growth of the Internet.

Again, I thank you for holding these hearings. I know how deeply you care about these issues and I hope we will continue to work closely together on many more of them.

[The above mentioned letter follows:]

GRAND LODGE, FRATERNAL ORDER OF POLICE,
LEGISLATIVE OFFICE,
Washington, DC, March 16, 2000.

The Hon. CHARLES E. SCHUMER,
U.S. Senate, Washington, DC.

DEAR SENATOR SCHUMER, I am writing this letter on behalf of the more than 285,000 members of the Fraternal Order of Police to advise you of our support for S. 2092. This legislation aims to help law enforcement fight high tech computer crime by amending Federal law.

Computers and high tech gadgetry are the newest tools of today's criminal, and law enforcement has not kept pace with the latest advances in crime. Your legislation will provide law enforcement with nationwide trap and trace authority, obviating the need to obtain a tap and trace order in each jurisdiction through which an electronic communication is made. Current technology, which can bounce electronic messages all around the world, often makes this an impossible task. This bill would reduce the requirement to a single order, allowing law enforcement to completely trace the communication to its source.

Currently law requires proof of damages in excess of $5,000 before Federal jurisdiction can be asserted. Your bill would amend the Computer Fraud and Abuse Act, allowing Federal prosecution of criminals from the outset—without having to wait for an assessment as to the amount of the damage inflicted. Any unauthorized, intrusion into critical infrastructure systems pose a significant risk to public safety and should be handled expeditiously as serious crimes.

This legislation also modifies an earlier directive to the sentencing commission, which required a six month mandatory prison sentence for certain violations of 18 U.S.C. 1030. While the F.O.P. believes all violations should be punished, the sentence requirement applies to some misdemeanor charges, even when the attack caused no damage. For this reason, prosecutors are often reluctant to bring any charges. The bill also amends section 1030 to give Federal law enforcement authorities the power to investigate and prosecute juvenile offenders for computer crimes when the. U.S. Attorney General certifies that such prosecution is appropriate.

These are modest but important changes to existing, law which will empower law enforcement to deal appropriately with the new computer criminal. I would like to commend for your leadership on this important issue and look forward to working with you and your staff to get this bill passed. If I can be of any further assistance, please do not hesitate to contact me or Executive Director Jim Pasco at my Washington office.

Sincerely,

GILBERT G. GALLEGOS,
National President.

Senator KYL. Thank you very much, Senator Schumer.

Our first witness today, as I said, is Louis Freeh, the Director of the Federal Bureau of Investigation. He is the principal administration official responsible for coordinating Federal law enforcement's efforts to protect our Nation's critical information infra-

structure. This coordination takes place at the National Infrastructure Protection Center, or NIPC.

Director Freeh, we will place your full written statement in the record and invite you to make any summary remarks you would like at this time. We are honored to have you here.

STATEMENT OF HON. LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. FREEH. Thank you very much, Mr. Chairman, Senator Feinstein, and Senators Schumer and Grassley. It is a pleasure and a privilege to be here before you. I can't think of a more timely and more critical inquiry for this Congress and for this country than all of the issues which you have collectively and correctly identified. Let me also thank you, Senator Kyl, Senator Feinstein, and Senator Schumer, for your leadership in this area.

A couple of points I would like to make, if I might, please, and you have a much more detailed statement for the record. I think Senator Schumer's point deserves some repetition. We are in a period of extraordinary change. We had a presentation given to my senior staff last week by the senior vice president of the largest manufacturer of technical computer equipment in the world, and what he said was that their company is now on an 18-month cycle of change; that is, every 18 months not only their equipment but the networks that support it and the corresponding infrastructures are changing, which means getting ready for the next 18 months is too late to prepare for these changes.

The FBI agents who are graduating from our academy now, in addition to receiving their firearms and their badge and credentials, receive a laptop computer. It is symptomatic of the venues in which they are going to work, a place and time of extraordinary change.

And if I could just, by illustration, give a couple of examples—some of them you know well—a subject in Russia, in St. Petersburg, using a laptop computer breaks into the largest U.S. bank, moves $10 million out of other people's accounts into his own accounts before the bank or anyone else is aware of that particular movement; $400,000 is lost. Thanks to our liaison in Russia and the United Kingdom—Senator, you mentioned the necessity of foreign cooperation—we were able to deal with that and resolve the matter.

Another individual in Sweden, 17 years old, breaks into Florida networks and shuts down 911 systems in a series of towns, depriving people of public safety as well as basic ambulatory concerns.

Three weeks ago, our office in New Haven notices on an Internet bulletin board the following statement made by an unidentified subscriber, ''Sometimes I feel like shooting up my school.'' The office in New Haven communicated that information back to our headquarters. Working with the tools and abilities that you have given us and the legal authorities that we have, we traced the message and messenger back to a small town in Canada. Using our liaison with our Canadian authorities, they seek out under their own laws and find and interview a 14-year-old subject who says, among other things, that he has access to explosives. They do, in fact, find dynamite, firearms, and in the words of the Canadian authorities,

this particular situation was very, very grave and discovered by using tools and using expertise transferred to an area of great change.

We have, since 1998, as you probably know, doubled the number of computer intrusion cases worked and opened in the FBI, from 547 to 1,154. In some of the areas where we work in cyber crime, such as the Innocent Images project which, as you know, is a project devoted to identifying and apprehending pedophiles who use the Internet not just to send child pornography, but more egregiously make arrangements directly with minors all over the world to meet them for illicit sexual purposes and travel interstate, violating our Federal statutes in that process, 497 new cases opened just in 1999, 193 arrests, 108 convictions, one typical area where, again, the people in the FBI, using these tools and resources, are dealing with a completely new phenomenon.

The National Infrastructure Protection Center, as you noted, Mr. Chairman, opened in February 1998. We have experienced a 39-percent increase in pending cases just in the computer intrusion area. A few days ago, the Computer Security Institute released its fifth annual Computer Crime and Security Survey. Ninety percent of its respondents report intrusions in the last 12 months, 74 percent reporting theft of property, intellectual information, commissions of intellectual property theft, financial fraud to the tune of $56 million, information theft to the tune of $68 million.

We are looking at the entire menu of computer crime, including the hacking phenomenon. We find that most of the unauthorized access cases are, in fact, done by insiders in companies, universities, government agencies. Seventy-one percent of the unauthorized access cases are committed, in fact, by insiders.

We had in 1997 a case where an individual who was disgruntled shut down the Forbes, Incorporated, computer systems for several days, causing extensive damage. In January and February 1999, the National Library of Medicine computer system which is relied upon by hundreds of thousands of doctors and medical professionals around the world was shut down again due to the sabotage of an insider. The FBI investigation identified the subject who was convicted in December.

With respect to the hacker phenomenon, several of you have mentioned the February 7 attacks, which demonstrated really the ease and the availability of such a devastating attack done still by very, very difficult and complex means, subject to the investigation that we are now trying to use to unravel it.

Politically-motivated attacks are also a large phenomenon. We have seen that, as you mentioned, Senator, in the Department of Justice, at the FBI, in fact. We have seen it at numerous companies and institutions all across the United States. The virus writers have also been an instrumental part of this comprehensive compromise of computer systems and networks. The Melissa Macro Virus case is a very, very good example of that. That investigation began with the virus spreading into our country's computer networks.

The Infrastructure Protection Center sent out warnings as soon as we had solid information about the virus and its impacts. These warnings, in fact, helped to alert the public and reduce the poten-

tial destructive impact of the virus. We received a tip from the New Jersey State Police, which in turn received a tip from America Online, and that followup resulted in the arrest of a subject, David Smith, on April 1, 1999, who has pled guilty and stipulated to actions which affected 1 million computer systems, causing $80 million in damages, and that is typical of the potential damage in these types of cases.

With respect to criminal groups, a whole separate sub-category of computer crime and hacking activities. We saw in the Phonemasters case, which was an FBI case worked last year, the ability of a small group of technically sophisticated criminals penetrating computer systems at MCI, Sprint, AT&T, Equifax, and even our own National Crime Information Center.

Under judicially-approved electronic surveillance orders, our office in Dallas was able to use intercept technology to monitor their calling activity, unravel their network, and was able finally to result in arrests and prosecutions. The methodology used by this group was called dumpster diving, gathering old phone books and technical manuals for computer systems and using that information then to break into the victims' systems—old-fashioned tools used in a new environment. I mentioned the Levin case, which was the theft and movement of $10 million out of our largest U.S. bank resulting in a loss of over $400,000.

We have seen terrorists using this technology and this venue to launch attacks. The Director of the Central Intelligence Agency testified recently that terrorist groups, including Hizbollah, Hamas, the Abu Nidal organization and, of course, Bin Laden's Qa'ida organization, are using computerized files, e-mail, and encryption to support their operations.

In the prosecution of Ramzi Yousef, who was convicted for the attack against the World Trade Center, as well as a plan to blow up American airliners in the Western Pacific, part of his very detailed plans to destroy those airliners was found on a laptop computer he used in the Philippines which was in an encrypted file and it made it very, very difficult to retrieve.

Foreign intelligence services are using this particular technology very effectively against the United States as well as our friends. The whole information warfare area which is being worked on by not just the FBI but our Department of Defense and the entire Government, as well as the governments of our allies, presents whole new challenges to national security. Internet fraud and all of the other aspects of this technology are becoming much more challenging than anybody contemplated a very short time ago.

We have taken some steps to deal with these issues and give us the ability to remain competent in this area. The one point I would like to make, echoing Senator Schumer remarks, is although we are in a period of extraordinary change and challenge with respect to technology, we are not asking for extraordinary powers. We are not asking for any more authorities than are currently contemplated under the Constitution and the Bill of Rights.

What we would like to do is maintain the balance that the Framers struck in 1792 when the fourth amendment was passed, which means that the expectation and the privacy of people in their homes and papers has to be secure, has to be paramount. But that

privacy can be breached when a neutral and detached magistrate finds by probable cause that a person or the place the person is using is committing a crime or about to commit a crime, and the constable on that finding is allowed to use authorized powers and authorities to protect public safety and enforce the laws.

We are seeking to maintain that balance and those authorities in a very complex and a very changing environment, but we are not asking for extraordinary powers. Indeed, nothing in the Schumer-Kyl bill does anything except keep us really at pace with these enormous and phenomenal changes.

We are working very closely with the private sector. This is a key area of our success. As you have mentioned, a lot of the response and a lot of the responsibility for dealing with these issues will fall to the private sector, the potential victims of many of these crimes.

I spoke very recently to the head of one of the largest police organizations in the world outside the United States and what he told me was somewhat sobering. He said that they did not have within his organization, a very sophisticated police organization, the means to do forensic computer investigations, analysis, and warning. And when the national companies were coming to him asking for help, he would say to them, "You go conduct the investigation, bring us the results, and then we will look at it in terms of making a prosecution decision or a charging decision."

I think that is a very bad policy for a government, and I think that it is incumbent upon the law enforcement authorities to have the capability and the competence to conduct those investigations under our authorities and to make the decisions and initiate work that will allow us to protect people and business in this critical area.

We should not be relegated to using contractors outside the Government for the basic investigative competence that we need, which is one of the reasons we have partnered, for instance, with the National White Collar Crime Center to set up an Internet fraud complaints center, which is an online complaints center where we can receive from the public and from industry complaints, referrals, and then make sure that if it is not a matter to be worked by the Federal Government or the FBI, we can delegate that to the State and local authorities that have that responsibility. We should be open and fully operational by May 8 of this year.

With respect to the distributed denial of service attacks, again, those are cases of immense importance to the country and to the FBI. We have a number of our major field offices directly and completely engaged in that investigation, coordinated by the National Infrastructure Protection Center back in Washington.

We are asking to set up an intellectual property protection center which would be partnered between the FBI and the Customs Service to again provide another channel for dealing with these complaints and effectively discharging our responsibilities in terms of investigations.

With respect to the legal authorities, you have all commented very eloquently on the aspects of the current state of the law which are impeding us and those very modest changes which would give us the advantages of technology to fight technology-type crimes.

The jurisdictional limit with respect to the pen registers is obviously a critical aspect of that modification.

It wouldn't make any sense, particularly in a Federal system, to go from State to State or county to county following a fugitive, getting a new fugitive warrant in each of those jurisdictions as the fugitive transitted the United States. We would have one Federal warrant and that would be good and viable in any parts of the U.S. jurisdiction where that person could be found or could be located.

With respect to pen registers and trap and trace orders, again I think the technology certainly was not contemplated under the current authorities, and that is, I think, a very modest but very critical improvement that would give us the ability to pursue things.

With respect to the damage limit, I think aggregating the damages and not looking for one single instance of a $5,000 limitation will greatly improve our ability. The use of administrative subpoenas, as we have found in other cases, particularly the health fraud cases, would give us the ability, under the supervision of the U.S. Attorneys' Offices, to conduct inquiries in a much more efficient manner, and one which is particularly suitable to cyberspace and crimes involving computers as well as the Internet.

The other aspects of the bill, I think, are not only prudent but necessary if we are to have a viable and effective response to what is a huge proliferation in hacking cases and crimes generally committed using the Internet and using the facilities of computers. We believe that these are modest changes not giving us any extraordinary powers, but giving us, we think, the power and the ability to remain effective and remain competent.

With respect to the other matters that the committee has been looking at in the context of that bill, again I want to just commend you, Mr. Chairman and the members of this committee, for your leadership in this area. We need to strive particularly in the years ahead to maintain our competence and our capability in an area which is changing faster than anybody contemplated a short time ago. So I very much appreciate your time and your attention and your leadership here, as well as the availability of this forum to discuss these very important issues.

Thank you.

Senator KYL. Thank you very much, Director Freeh. There is much in your written statement that you haven't commented on orally, but you noted many other examples in your written statement of attacks on our information infrastructure in a whole variety of situations and those bear our attention as well.

You noted, for example, that a Kevin Mitnick evaded attempts to trace his calls by moving around the country and by using cellular telephones which routed calls through multiple carriers on their way to a final destination, and it was impossible to get orders in each of those places quickly enough in order to trace the calls. So it is not as if people who are intending to violate the law don't understand fully the hoops that the law enforcement people have to jump through in order to trace them.

Let me just begin by asking you a question about resources. Attorney General Reno testified earlier this year that the Administration was requesting $37 million in funding enhancements for cyber crime prosecution and investigation. But given the increasing

workload that you face that you have testified to here today, is this funding level sufficient, or should Congress look to increase this level in the annual funding bills that we are going to be debating soon?

Mr. FREEH. I think it is a good initiative and a good start, but not adequate to deal with the comprehensive nature of this problem, as well as the accelerated growth. For instance, part of that funding which is very, very critical for us is an increase by 100 of our computer examiners; we call them our card examiners. These are the men and women in the FBI who go to the hard drives, who extract forensically evidence and maintain it in a way that is presentable in a court of law.

The number of examinations have gone from 1,800 a year ago to what we estimate next year will be 6,000 examinations. Half of our cases now routinely have computer examination requirements, and that is likely to accelerate. But the total package that you refer to does not begin to address the National Infrastructure Protection Center enhancements, issues regarding encryption, issues regarding computer squads, 16 of them now active throughout the FBI, Los Angeles, CA, being an example, but squads which are now in huge demand not just in the FBI but on State and local requests.

We spoke before the hearing, Senator Feinstein and I, about an initiative which we put forward in San Diego which was the first establishment of a computer forensic lab which is staffed not just by FBI examiners but by State and local scientists. And the reason for that is quite simple. First, to bring everything back to Washington for examination just doesn't make any sense, particularly in an electronic age dealing with electronic evidence.

Second, it is important that we begin to grow and cultivate State and local expertise in these areas. The laboratory in San Diego was stood up at a very, very modest cost, but gives tremendous capability to the law enforcement community, not just the Federal community, in that area. There is a whole bunch of other places around the country where this is in huge demand, and those are some of the resources that could certainly be well used.

Senator KYL. Thank you very much. Senator Feinstein notes that the air conditioning here is obviously not working. If you would like to shed your jacket, as I did, you are welcome to do that. I know you are very warm.

Let me just ask you one other question, in deference to the other people who are on the dais, and I note that Senator Bennett from Utah has joined us. Senator Bennett, of course, chaired the Y2K Committee and has maintained his leadership as one of the people called upon by our leadership to coordinate efforts of the various committees with jurisdiction to deal with the variety of issues that we are facing. I am glad, Senator Bennett, that you have joined us here.

Director Freeh, in your testimony you noted your desire for the FBI to have the authority to issue administrative subpoenas. As I noted earlier, companies are reluctant to share information on cyber crimes with law enforcement officials because public disclosure of such intrusions could lead to lost sales and a decline in a company's stock price.

What checks and balances would be used to ensure that information acquired through administrative subpoenas would remain confidential and that such subpoena power would not be abused by the FBI?

Mr. FREEH. Several things, Mr. Chairman. First of all, a lot of the information that would be obtained from administrative subpoenas would be part and parcel of the criminal investigation, which would also in most cases at least at a certain stage become part of a grand jury process. The administrative subpoena process would be ancillary to, in most cases, a grand jury process, which would give it adequate secrecy and afford confidentiality.

The discovery of that particular material, at least in terms of litigation or prosecution, would really be equivalent to any information or testimony actually taken in a grand jury. The same discovery process under rule 16 would have to occur. Protective orders could be sought and routinely would be sought during that discovery process.

It would have the protections of the Privacy Act and the Freedom of Information Act. So, that information would be used in a confidential manner ancillary to a criminal inquiry and in many cases would become part and parcel of a grand jury. It would be supervised and controlled by the U.S. attorney and the availability of that information, in my view, is limited in many respects as the grand jury information.

Senator KYL. I think that is an extremely important point because there is some reluctance on the part of some people in the private sector to acknowledge intrusions into their systems and to share information with law enforcement because of their fear that this could hurt them commercially.

My own view is that they need to understand that the involvement of law enforcement is their biggest protection, for precisely the reason that you just noted. Once it is in that context, the information can, in fact, be protected from public disclosure, in the interest of that commercial enterprise, and also in the interest of the prosecution. So I think this is an important point for all of us to stress as we urge greater cooperation with the private sector and our law enforcement.

Mr. FREEH. Senator, I might also mention that under the Economic Espionage Act which this Congress passed in 1996, there are particular and specific provisions for confidentiality in the process of a criminal prosecution or discovery. That is very important for corporations to understand because if their proprietary information is at risk or in some cases has been taken, of course, there is a corporate fear, as there should be, that reporting that to the FBI is going to make matters worse because the trade secret is going to become disclosed in the course of the investigation.

But that statute, the economic espionage statute, particularly, even beyond the grand jury protections of rule 6(e), gives specific and court-ordered protection to those trade secrets so they are not compromised in the course of a prosecution, and we pay very, very close attention to that.

Senator KYL. A very, very important point.

Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Mr. Freeh, in your written remarks you mention that technology has moved so fast and yet our laws have not been able to keep up with that technology. You point out on page 9 that you are working with Justice to propose a legislative package for our review to keep laws in step. I wanted to ask you when that would be ready.

You also point out that the FBI does not have the authority to issue administrative subpoenas while conducting investigations involving Internet fraud, and you detail why an administrative subpoena would be useful and also protect due process of law. You also point out that many laws were not drafted in a technologically neutral way and don't make a lot of sense, and that goes into the pen register trap and trace statutes, et cetera, et cetera.

When will you have that package ready? I was looking at some of the sentences in the cases, particularly the Phonemasters case as well as the St. Petersburg case. I mean, really, this is major robbery—well, it is not robbery because I guess it is not a crime against a person. But you have $10 million thefts that occur, with a lot of criminal conspiracy, and yet individuals will get in terms of a sentence maybe just 3 years.

Are you looking at a revision of the codes with respect to this, and when will your recommendations be available?

Mr. FREEH. Senator, I will get back to you, if I might, on the date. I know this is a matter being worked not only by the Department of Justice but we have certainly contributed some input to that.

My view is—and I have testified about this before—that the penalties really need to be reviewed, and reviewed exactly along the lines that you suggest in your question. Under the racketeering statute which is used, I think, very judiciously by the Government in a criminal context, two acts of mail or wire fraud could constitute under the appropriate circumstances an enterprise engaged in racketeering activity, which would then make the convicted subjects eligible to very severe penalties—20 years in prison, forfeitures, damages, et cetera, et cetera.

If you overlay that set of requirements with the type of cases that we have seen here and cases where literally you could crash not only a number of Internet companies but cause millions of dollars in damages, and you could crash power grids, hospital records, and actually cause great injury or death or extreme damage to individuals or property, I think again the statutes that are drafted with a 3- to 5-year penalty in mind just don't contemplate, nor could they when they were enacted, I think, the scope and the potential of the damage.

So I think that that is a fair matter for the Congress to review and I think, as with the racketeering statute, you can set guidelines and requirements, including specific Department of Justice review procedures, so this is not used willy-nilly. This is not something that I am suggesting should be used in even routine or nonroutine hacking cases. But it occurs to me, given some of the matters that we are looking at, that there is an area of extreme damage and threat here that really can't be properly or even fairly compared with a 3- to 5-year criminal exposure.

Senator FEINSTEIN. So in other words, what you do is amend the predicate statutes and add some of these crimes. Having just done

this in the Gang Abatement Act in our juvenile justice bill, and looking at a lot of predicate statutes, they really don't relate to this. So you would have to add, I think, those statutes to apply the RICO statutes.

Mr. FREEH. Yes, that could be done. The Congress has done that consistently since 1968 as new crimes have become important to deal with.

Senator FEINSTEIN. Right.

Mr. FREEH. And I think this is a very appropriate one to consider.

Senator FEINSTEIN. I would be most interested in that because I don't think our criminal statutes keep up at all with the kind of conspiracy that is involved with this, and also the literal power that it is to take down entire institutions. I think that has to be taken into consideration when drafting criminal codes.

Could you comment on the need for administrative subpoenas?

Mr. FREEH. Yes; we use them now. Let me just give you one example where the Congress has authorized us to use them, going back now to 1996 in the healthcare fraud area. And in that area of investigation, it is very similar to cyber crime where huge amounts of materials have to be reviewed, particularly logs in the computer case; in the healthcare fraud area, literally hundreds of thousands of records and documents.

It is very important in many cases that not just the criminal investigators view these materials but that the noncriminal investigators, the scientists in the healthcare area, doctors and medical professionals, are able to get access to that information in a very controlled setting, but to get the information quickly, to get it comprehensively, to be able to review very rapidly a fast-moving criminal or noncriminal event using computers in cyberspace.

So I think what it does is it gives the Government investigators more efficiency, more speed, without compromising the confidentiality as well as the security that that information would receive. But it has been used very effectively in the healthcare area. It could probably be used more effectively in this area because the volumes of logs that are required to be reviewed and the number of different experts that need to look at that, including people who are not criminal investigators, really lends itself to an administrative subpoena context which I think would be appropriate here.

Senator FEINSTEIN. Some in the industry have argued that companies will not share information with law enforcement regarding cyber attacks because much of the information is proprietary and sensitive in that regard, and they are afraid that the Government will leak or otherwise disclose that information which would benefit competitors.

Do you support a FOIA exemption for industry, say one prohibiting public access to information that companies provide the National Information Protection Center regarding cyber attacks?

Mr. FREEH. I would certainly tend to favor it in the limited area of trade secrets, proprietary information, intellectual property, much like my comments about the Economic Espionage Act where that is carved out as an area that protects things that are critical to conduct an investigation but would be devastating economically and otherwise to the owner of that property if it was disclosed or

made publicly available. It would defeat the purpose of the investigation, which is to protect that property if, in fact, that process leads to the disclosure to competitors and others of trade secrets, legitimate intellectual property that needs to be protected. So I would think that is a very fair and traditional area to carve out protections for.

Senator FEINSTEIN. Would that be part of the package that you will submit?

Mr. FREEH. It will certainly be part of our recommendations, but I haven't seen the final workout because the Department of Justice has the lead in drafting that. But let me see if I can get back to you and inform you on that.

Senator FEINSTEIN. I appreciate that. Thank you. Thanks very much.

Senator KYL. Thank you, Senator Feinstein.

Senator Grassley.

Senator GRASSLEY. Thank you, Director Freeh, for your appearance here and, most importantly, keeping ahead of the problems that law enforcement faces. I know with a high-tech society it is very difficult.

I want to refer to the presidential directive that established the National Infrastructure Protection Center. It stated that the Center would include representatives of the FBI, Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives from the Department of Defense, intelligence community, and lead agencies.

It is my understanding, Director Freeh, that there are about 19 agencies that were originally assigned to the NIPC as partners with the FBI. Is it true that there are only five agencies now remaining in the NIPC, and why are there only five?

Mr. FREEH. We have about 11 agencies that are currently participating with detailees, but you are correct; we do not have all of the representation contemplated in the order. Most importantly, we are still trying to obtain representatives from the Department of the Treasury and the Department of Commerce, two very key components in this sector, and that is a process that continues. But we do have the participation of the other agencies that I mentioned and they have been working on a full-time basis to further the goals of that Center.

Senator GRASSLEY. You didn't say this, but is there an inference that you are working to get the cooperation of these agencies, that there are turf problems or some foot-dragging on the part of other departments and bureaucracies that ought to be cooperating with you and aren't cooperating with you?

Mr. FREEH. I think part of it, Senator, is the high premium that these resources have. The Department of the Treasury and the Department of Commerce have their own computer centers, their own obligations and requirements in terms of investigations. So they have had trouble providing resources to what is a brand new initiative and one which is different from their own individual responsibilities. So we need to work better to bring this Center to fruition.

Senator GRASSLEY. Maybe we shouldn't assume that there might be some sort of lack of cooperation on the part of those departments.

Let me ask you this. If those departments were fully cooperating with you so that all 19, or at least a larger number of agencies would be cooperating with the NIPC, would that be a better rallying of resources of our Government than having the 11 agencies you have and then having 2 or 3 others out here concerned about it in another way?

Mr. FREEH. I believe that consolidating these resources and this expertise in one place, as the PDD you referred to contemplated, makes the most sense because this is the Center that not only conducts the investigations, but it is responsible for the threat warnings. The chairman mentioned one that was sent out last year in advance of the distributed attacks.

It does training, it does liaison with the private sector. It makes much more sense for a large corporate actor to hear from one representative, from the NIPC, than from three or four different government agencies or components. So it makes a lot of sense to consolidate it.

Senator GRASSLEY. Well, I know you haven't said this and I don't want to put words in your mouth, but I think that Congress' oversight responsibility to see that the laws are faithfully enforced and that the mandates are carried out as intended—that part of our oversight ought to be showing some concern because all of these resources aren't being brought under the same directorship. That is my statement. I am not asking you to agree with it, but if you would say you would agree, that would help us. It might help you, too.

Mr. FREEH. I think we have to make a better effort to consolidate these resources and put them in one place. There is no question but that that is a more efficient way to do what is very difficult to do just on its own terms, but to do it without all of the assets at one table makes it very, very burdensome.

Senator GRASSLEY. I want to go on now to your written testimony and, "The number of pending cases has increased from 39 percent, from 610 at the end of fiscal year 1998 to 834 at the end of fiscal year 1999." So my question: of the 834 pending cases, what percentage are being investigated by your partner agencies?

Mr. FREEH. I think those are the cases that are in the Center, in the NIPC itself. So what I would say is that the—and Mike Vatis will correct me if I am not accurate—that those are the cases which are subject to the Center's investigation, which is the collective effort of the agencies represented there.

Senator GRASSLEY. So then there might be some cases being investigated that you wouldn't know about by the agencies that are not cooperating under your directorship at this point?

Mr. FREEH. Yes; throughout the Government, I would assume that there would be other matters that are not known to the Center.

Senator GRASSLEY. Of your 1999 pending cases, how many would you say had a direct impact on national critical infrastructure protection and ability to predict indications of an attack, as compared to pending cases that are for the purpose of monitoring for study and possible future impact on the critical infrastructure?

Mr. FREEH. May I consult with Mr. Vatis on that?

Mr. Vatis, who is actually the director of the Center, says that we probably don't have that breakdown for you right here, but he thinks he can work on some analysis for you along those lines and get it back to you quickly.

Senator GRASSLEY. Thank you. I am done with my questioning.

Senator KYL. Thank you, Senator Grassley.

Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman, and you have covered almost all the questions I wanted to ask. I have two, one just elaborating a little bit on the international issue which we both touched on.

Cyber criminals, as you know, can cruise over international borders with complete ease, making the need for cooperation with foreign governments on crime matters greater than they have been in the past. I know you have been thinking about this, as has the Department of Justice. Can you give us your take on what holds for the future in this area? Are we talking to other governments? What kind of cooperation are we getting? What are the barriers, et cetera?

Mr. FREEH. We are talking to them, Senator, continuously and very, very comprehensively. In many of the cases that I have cited, and others which I have not cited, we would not have been able to get out of the starting gate without the assistance of our partners.

For instance, over the millennial periods, there were a series of events not just in the northwest United States but in the Mideast and even in the Far East that required the deployment of FBI agents, FBI computer examiners, who hooked up with our partners, liaison services in a number of different countries that gave us direct access to computer hard drives which in some cases were the actual plans of terrorists to murder large numbers of Americans.

Those methods of coordination and liaison are critical because the Internet has no sovereignty, has no boundaries, as we all know. We work very regularly with our partners overseas. We have had many of our liaison partners back to the United States. We have done extensive training through the NIPC to our foreign counterparts. They have set up similar computer centers. The idea will be to have these centers hooked up on a realtime basis and have standard protocols, as well as forensic examination standards.

So this is an area that is being pressed very hard not just by our agency but by our counterpart agencies around the world. I just came back from a trip to the Persian Gulf and I visited six countries there. Every one of the countries asked about computer crimes, looking for help and assistance in conducting investigations. We do international training to a large degree along these particular lines. So it is a huge area of growth and potential liaison.

Senator SCHUMER. So, overall, you are getting the cooperation you need from foreign governments in this?

Mr. FREEH. Yes.

Senator SCHUMER. Are there any particular governments or any regions where we are not getting that kind of cooperation, and do you get them not only on major cases like terrorism but on things that they might still regard as minor, such as DOS-type invasions?

Mr. FREEH. We get them on the terrorism cases, which are probably the most active component of that liaison. We get them also on the financial crimes cases. The Bank of New York case, which you are familiar with, is being worked not only by the United States as well as Russian authorities, but there are computer links and leads and evidence with respect to that matter which literally go all around the world which we are following up on. So it transcends terrorism into financial crimes, into even organized crime and drug trafficking areas. It has become part and parcel of what we do on a routine basis.

Senator SCHUMER. Any particular places, countries, governments where you are not getting cooperation—major ones?

Mr. FREEH. Not really. On a case-by-case basis, we have gotten extremely good cooperation.

Senator SCHUMER. My only other question is could you address the problem of juveniles committing computer crimes? Are there unique solutions we should be working on, are the laws adequate, et cetera?

Mr. FREEH. You know, it is a very serious problem. The case that I mentioned before, of course, involves a 14-year-old. Many of the matters that we are currently looking at in this area—cyber crime, the hacking cases—involve juveniles who are very adept and in many cases surprisingly competent in the acts that they commit and achieve.

I think what has to be done is two things. No. 1, there has got to be a strong educational component to what we do in terms of computer training and education. The whole notion of ethics as well as lawfulness with respect to the computer and the potential damage that this technology can cause in the wrong hands has to be something which becomes regularly instructed and part and parcel of our whole educational process, not just for juveniles, by the way. I think that we probably do a better job across the board in that area.

In the prevention area as well as the enforcement area, I think looking at the number of juveniles active in this area is going to require some adjustments or modifications, at least a serious review of the current statutory authorities which in most cases were written 50, 60 years ago, and the whole notion of juveniles in this type of endeavor and activity clearly not contemplated. So I think it is a combination of education and also some modification of the laws because there has to be some deterrent and some ability to achieve some results in that area.

Senator SCHUMER. Would you get to us some specific—or I guess you will have to work it through DOJ, but maybe you and they together, some specific recommendations on juvenile issues that are needed?

Mr. FREEH. Yes, I will.

Senator SCHUMER. Thank you. Thank you, Mr. Chairman.

Senator KYL. Thank you, Senator Schumer.

Senator Feinstein.

Senator FEINSTEIN. Mr. Chairman, may I have unanimous consent to place a statement by the ranking member in the record, please?

Senator KYL. Without objection, so ordered.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

As we head into the twenty-first century, computer-related crime is one of the greatest challenges facing law enforcement. Many of our critical infrastructures and our government depend upon the reliability and security of complex computer systems. We need to make sure that these essential systems are protected from all forms of attack.

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, Congressional buildings like this one use cement pillars placed at entrances, photo identification cards, metal detectors, x-ray scanners and security guards to protect the 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 recent hacker attacks 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 cyberattack on 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. We have learned that even law enforcement is not immune. Last month we learned of a denial of service attack successfully perpetrated against a FBI web site, shutting down that site for several hours.

The cybercrime problem is growing. 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 recent headline-grabbing "denial-of-service" attacks, 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 and made the following observations. 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."

I commend the FBI Director for establishing the Pittsburgh High Tech Computer Crimes Task Force to take advantage of the technical expertise at CERT to both solve and prevent newly emerging forms of computer network attacks. Senator Hatch and I are working together on legislation that would encourage the development of such regional task forces.

Cybercrime is not a new problem. 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 Senate 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 has 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.

Encryption helps prevent cybercrime. 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 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.

The private sector must assume primary responsibility for protecting its 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 defense is a good offense. Americans and American firms must be encouraged to take preventive measures to protect their computer information and systems. Just recently, internet providers and companies such as Yahoo! and Amazon.com Inc., and computer hardware companies such as Cisco Systems Inc., proved successful at stemming attacks within hours thereby limiting losses.

Prior legislative efforts were designed to deter cybercrime. 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, as well as the legislation that Senator Hatch and I are crafting, would help state and local law enforcement join the fight to combat the worsening threats we face from computer crime.

Our computer crime laws must be kept up-to-date as an important backstop and deterrent. I believe that our current computer crime laws can be enhanced and that the time to act is now. We should pass legislation designed to improve our law enforcement efforts while at the same time protecting the privacy rights of American citizens. Such legislation should make it more efficient for law enforcement to use tools that are already available—such as pen registers and trap and trace devices—to track down computer criminals expeditiously. It should ensure that law enforcement can investigate and prosecute hacker attacks even when perpetrators use foreign-based computers to facilitate their crimes. It should implement criminal forfeiture provisions to ensure that hackers are forced to relinquish the tools of their trade upon conviction. It should also close a current loophole in our wiretap laws that prevents a law enforcement officer from monitoring an innocent-host computer with the consent of the computer's owner and without a wiretap order to track down the source of denial-of-service attacks. Finally, such legislation should assist state and local police departments in their parallel efforts to combat cybercrime, in recognition of the fact that this fight is not just at the federal level.

I have been working with Senator Hatch on legislation to accomplish all of these goals and look forward to discussing these proposals with law enforcement and industry leaders.

Civil Fraud Laws May Also Need Strengthening. There is no question that fraud is one of the most pressing problems facing the Internet. According to the Director of the FBI, frauds have tainted Internet sales of merchandise, auctions, sweepstakes and business opportunities and the North American Securities Administrators Association estimates that Internet-related stock fraud alone results in billions of dollars of loss to investors each year. I understand that the FBI and the National White

Collar Crime Center are jointly sponsoring the Internet Fraud Complaint Center, which will help assist in the investigation of fraudulent schemes on the Internet and will compile data on cyber-frauds. I applaud this endeavor.

In looking for ways to combat Internet fraud, we should consider whether the Justice Department's authority to use civil enforcement mechanisms against those engaged in frauds on the Internet should be enhanced.

Legislation must be balanced to protect our privacy and other constitutional rights. 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 antisocial 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 thank Senators Kyl, Feinstein and Schumer for their attention to this important issue.

Senator KYL. Senator Bennett.

Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman, and I appreciate your courtesy and willingness to let me come in and participate in this with you. It is a matter of great personal interest. I realize that you, Mr. Chairman, and this subcommittee have done perhaps more in this particular issue than any other group in the Congress, with the possible exception of the efforts being expended in the Armed Services Committee as they deal with DOD issues. Most of the questions that I would have, have already been touched on.

Mr. Freeh, I would like to get your reaction to one issue. We as a Nation spent $15 million setting up the information coordinating center to deal with Y2K. It turned out to be a nonevent as far as the ICC was concerned, and a lot of people said, "Gee, why did you go to all that trouble? That is a fairly significant investment. The wiring is in the floor, the computers are in place," and so on.

Do you have any suggestions as to the future of that facility? Should it be dismantled and packed away, and say, "Gee, that was a bullet that missed us, so we can forget it?" Or do you see any utility for that facility long term in dealing with cyber crimes or even cyber warfare?

Mr. FREEH. Senator, I think, first of all, it was a good investment and a prudent one, given the threats that you particularly and others were responsible for analyzing and dealing with and predicting.

I would like to, if I might, just consider that a little bit and get back to you. I don't have any concerns about continuing the activity to the extent that it would complement and support other activities. I guess my concern, which was reflected in my answer to Senator Grassley, is that this is such a huge challenge and a huge burden that we don't want to split our forces before we then fielded our team.

And if we are going to be bifurcating responsibilities and taking what the PDD said the NIPC should be doing and assigning it to

another facility because the facility is available without some coordination or some overall administrative control by the people responsible for not just the criminal investigations but analysis, threat warning, training, liaison; the worse thing to do right now would be to split our forces because our forces are quite meager, given the challenges that we need to get geared up for.

Senator BENNETT. Well, I would appreciate any response that you might have. Some of us in the Congress have written to OMB and said that we think this facility should be maintained and turned over to CIAO. OMB thinks it should be dismantled and those portions that might be of some value should be handed over to FEMA.

I do not see the protection of critical infrastructure as a FEMA responsibility, and I think CIAO comes the closest as an agency to deal with that and one with whom you could coordinate very closely. So I don't seem to be able to influence OMB and I am putting you on something of a spot to ask your opinion on this, but I think the facility represents a relatively, if there is such a thing, unique asset, certainly a very rare asset.

It is unique in that nothing else has been created quite like it, and I want to see it utilized if there is any possibility that it can be utilized with respect to cyber crimes or cyber terrorism. So if you would respond, I would appreciate that.

Mr. FREEH. I will be happy to do that, Senator.

Senator BENNETT. Now, looking ahead at the testimony of the next witness, there is a paragraph that I would like to read to you out of his written testimony and just give you an opportunity to respond while you are here because very often you come, you leave, then he speaks and you don't get a chance to comment.

So in Mr. Harris Miller's testimony he says, "Few high-tech companies are interested in being perceived by their customers as active agents of law enforcement. Agencies, meanwhile, are often viewed as demanding this type of information from the private sector, but giving little back in return. Let me be blunt: information sharing cannot be a one-way street."

Would you like to comment on that statement? That is pretty blunt and I think opens the dialog in a useful way.

Mr. FREEH. Well, I certainly agree that in the responsibilities that we have as a law enforcement agency vis-à-vis the private sector, you cannot have a one-way street. The information can't just be flowing from the private sector to constable. It just doesn't make any sense.

What I would say is that in a general and maybe broader context—and this has been echoed by other members of the committee—law enforcement and public safety and protection of property in this area, except for the technology, is really not different from what law enforcement traditionally has done for a long time, over 200 years just in this country.

We cannot unilaterally protect these companies, the information, the people who work there, the jobs, as well as the economic security that flows from a robust private sector without their assistance, no more than they can protect in the course of civil litigation or injunctions or market leverage—they can't protect their property

without the help, when appropriate, of the enforcement agencies and the power of the State or the criminal courts.

So it is a necessary marriage. There is a critical need for there to be not only information sharing but cooperation. Now, that requires work on both sides. We have to respect, as we mentioned before, the confidentiality as well as the value of the information and secrets that they may give to us to do our job.

On the other hand, they have to be willing to report to the authorities incidents of crime, as banks are required to do by statute. They have to come to us when they are the subjects of an extortion or a threat, when someone steals their trade secret, rather than just trying to work on it themselves. It can't be done unless information is flowing in both directions, which is why the Information Infrastructure Protection Center as one of its primary responsibilities under the PDD is to have an active, robust and credible liaison with the private sector. We can't operate without that.

Senator BENNETT. Thank you. I think that is useful and I appreciate your adding that to the record. Following up with one specific of the questions that Senator Schumer raised, the Toronto Star reported on Sunday that approximately 80 percent of the foreign attacks on U.S. computer networks either originate in or pass through Canada.

You talked about your relationships in the world generally. Could you give us an update on the status of United States and Canadian cooperation in this area?

Mr. FREEH. Yes; I would say the status of that cooperation is really excellent. During the millennial period, particularly when we were working with respect to the events out in the Northwest, both from the criminal justice point of view but also from the intelligence and investigative point of view, you would not find anyplace in the world a closer integration or cooperation.

FBI agents were in Canada, RCMP officers were in the United States, in many cases drafting applications for court authorities in both countries together; realtime feedback of information, sharing of information obtained from searches with appropriate court disclosure orders. That relationship is almost a seamless one not only in the cyber areas but in generally all criminal justice areas, in the counterterrorism area, and that is probably one of the best relationships between countries on those issues as anyplace I have seen.

Senator BENNETT. Thank you very much, and thank you, Mr. Chairman, for allowing me to participate. I appreciate it.

Senator KYL. Thank you, Senator Bennett. As always, your intervention is very helpful.

Director Freeh, we could question you all morning, I am sure, and be much better edified than we are, but we have another panel and I think we will call upon them. We appreciate very much your continued diligence in dealing with this area. We will try to help get the resources to you that you need. You have certainly helped to create the case for further legislation that we want to pursue here, and so we thank you very, very much for being with us this morning and wish you well.

Mr. FREEH. Thank you, Mr. Chairman, and thank you both for your leadership in this area.

[The prepared statement of Mr. Freeh follows:]

PREPARED STATEMENT OF LOUIS J. FREEH

Good morning, Mr. Chairman, Senator Feinstein, and Members of the Subcommittee. I am privileged to have 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. The recent denial of service attacks on leading elements of the electronic economic sector, including Yahoo!, Amazon.com, Buy.com, Ebay, E*Trade, CNN, and others, had dramatic and immediate impact on many Americans. As Senator Bennett recently stated, "these attacks are only the tip of the iceberg. They are the part of the iceberg that is visible above the water-in clear view. But as everyone knows, the largest part of the iceberg, and possibly the most dangerous, lies beneath the surface of the water and is difficult to detect. This is true also with the range of threats to the Internet and those that rely upon it."

I would like to acknowledge the strong support this Subcommittee has provided to the FBI over the past several years for fighting cybercrime. Senator Kyl's strong support for vital cyber crime legislation such as the National Infrastructure Protection Act of 1996 and the Schumer-Kyl bill strengthening 18 U.S.C. § 1030, is greatly appreciated. Senator Kyl and this committee have also been the strongest supporters of our National Infrastructure Protection Center. 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 highlight some recent cases Then I will comment on our use of 18 U.S.C. § 1030 in fighting cybercrime and say a few words about the Schumer-Kyl bill. 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 1154. 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.

A few days ago the Computer Security Institute released its fifth annual "Computer Crime and Security Survey." The results only confirm what we had already suspected given our burgeoning case load, that more companies surveyed are reporting intrusions, that dollar losses are increasing, that insiders remain a serious threat, and that more companies are doing more business on the Internet than ever before.

The statistics tell the story. Ninety percent of respondents detected security breaches over the last 12 months. At least 74 percent of respondents reported security breaches including theft of proprietary information, financial fraud, system penetration by outsiders, data or network sabotage, or denial of service attacks. Information theft and financial fraud caused the most severe financial losses, put at $68 million and $56 million respectively. The losses from 273 respondents totaled just over $265 million. Losses traced to denial of service attacks were only $77,000 in 1998, and by 1999 had risen to just $116,250. Further, the new survey reports on numbers taken before the high-profile February attacks against Yahoo, Amazon and eBay. Finally, many companies are experiencing multiple attacks; 19 percent of respondents reported 10 or more incidents.

Over the past several years we have seen a range of computer crimes ranging from defacement of websites by juveniles to sophisticated intrusions that we suspect may be sponsored by foreign powers, and everything in between. Some of these are obviously more significant than others. The theft of national security information

from a government agency or the interruption of electrical power to a major metropolitan area have greater consequences for national security, public safety, and the economy than the defacement of a web-site. But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A website hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce. Because of these implications, it is critical that we have in place the programs and resources to investigate and, ultimately, to deter these sorts of crimes.

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

Insiders. The disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies. Insiders' knowledge of the target companies' network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The just-released 2000 survey by the Computer Security Institute and FBI reports that 71 percent of respondents detected unauthorized access to systems by insiders.

One example of an insider was George Parente. In 1997, Parente was arrested for causing five network servers at the publishing company Forbes, Inc., to crash. Parente was a former Forbes computer technician who had been terminated from temporary employment. In what appears to have been a vengeful act against the company and his supervisors, Parente dialed into the Forbes computer system from his residence and gained access through a co-worker's log-in and password. Once online, he caused five of the eight Forbes computer network servers to crash, and erased all of the server volume on each of the affected servers. No data could be restored. Parente's sabotage resulted in a 2-day shut down in Forbes' New York operations with losses exceeding $100,000. Parente pleaded guilty to one count of violating of the Computer Fraud and Abuse Act, Title 18 U.S.C. § 1030.

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 passswords 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 (or "crackers") are also a common threat. They sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes.

While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. The distributed denial-of-service (DDOS) attacks last month are only the most recent illustration of the economic disruption that can be caused by tools now readily available on the Internet.

Another recent case illustrates the scope of the problem. On Friday authorities in Wales, acting in coordination with the FBI, arrested two individuals for alleged intrusions into e-commerce sites in several countries and the theft of credit card information on over 26,000 accounts. One subject used the Internet alias "CURADOR." Losses from this case could exceed $3,000,000. The FBI cooperated closely with the Dyfed-Powys Police Service in the United Kingdom, the Royal Canadian Mounted Police in Canada, and private industry. This investigation involved the Philadelphia Division, seven other FBI field offices, our Legal Attache in London, and the NIPC. This case demonstrates the close partnerships that we have built with our foreign law enforcement counterparts and with private industry.

We have also seen a rise recently in politically motivated attacks on web pages or e-mail servers, which some have dubbed "hacktivism." In these incidents, groups

and individuals overload e-mail servers or deface websites to send a political message. While these attacks generally have not altered operating systems or networks, they have disrupted services, caused monetary loss, and denied the public access to websites containing valuable information, thereby infringing on others' rights to disseminate and receive information. Examples of "hacktivism" include a case in 1996, in which an unknown subject gained unauthorized access to the computer system hosting the Department of Justice Internet web site. The intruders deleted over 200 directories and their contents on the computer system and installed their own pages. The installed pages were critical of the Communications Decency Act (CDA) and included pictures of Adolf Hitler, swastikas, pictures of sexual bondage scenes, a speech falsely attributed to President Clinton, and fabricated CDA text.

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

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

Criminal Groups. We are also seeing the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. In September, 1999, two members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized—access devices (18 USC § 1029) and unauthorized access to a federal interest computer (18 USC § 1030). The "Phonemasters" were an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the National Crime Information Center. Under judicially-approved electronic surveillance orders, the FBI's Dallas Division made use of new data intercept technology to monitor the calling activity and modem pulses of one of the suspects, Calvin Cantrell. Mr. Cantrell downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Cantrell was sentenced to 2 years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

The Phonemasters' methods included "dumpster diving" to gather old phone books and technical manuals for systems. They used this information to trick employees into giving up their logon and password information. The group then used this information to break into victim systems. It is important to remember that often "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.

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

Beyond criminal threats in cyber space, we also face a variety of significant national security threats.

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

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

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

The categories described above involve computers used as weapons and as targets of a crime. We are also seeing computers used to facilitate more traditional forms of crime.

Internet Fraud. One of the most critical challenges facing the FBI and law enforcement in general, is the use of the Internet for fraudulent purposes. Understanding and using the Internet to combat Internet fraud is essential for law enforcement. The accessibility of such an immense audience coupled with the anonymity of the subject, require a different approach. The Internet is a perfect medium to locate victims and provide an environment where victims do not see or speak to the "fraudsters." Anyone in the privacy of their own home can create a very persuasive vehicle for fraud over the Internet. Internet fraud does not have traditional boundaries as seen in the traditional schemes. The traditional methods of detecting, reporting, and investigating fraud fail in this environment. 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.

Let me provide you with some specific examples. Securities offered over the Internet have added an entirely new dimension to securities fraud investigations. Investors are able to research potential investments and actually invest over the Internet with ease through electronic linkage to a number of services that provide stock and commodity quotations, as well as, critical financial information. The North American Securities Administrators Association has estimated that Internet-related stock fraud results in approximately $10 billion per year (or $1 million per hour) loss to investors, this is currently the second most common form of investment fraud.

On April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in

Tustin, California. An e-mail posted on the message board under the subject line "Buyout News" said that PairGain was being taken over by an Israeli company. The e-mail also provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly-traded stock shot up more than 30 percent, and the trading volume grew to nearly seven times its norm. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial losses to many investors who purchased the stock at artificially inflated prices.

Within a week after this hoax appeared, the FBI arrested a Raleigh North Carolina man for what was believed to be the first stock manipulation scheme perpetrated by a fraudulent Internet site. The perpetrator was traced through an Internet Protocol address that he used, and he was charged with securities fraud for disseminating false information about a publicly-traded stock.

In another example, on March 5, 2000 nineteen people were charged in a muitimillion-dollar New York-based inside trading scheme. In one of the first cases of its kind, the Internet took a starring role as allegedly about $8.4 million was illegally pocketed from secrets traded in cyberspace chat rooms. Richard Walker, director of enforcement for the Securities and Exchange Commission, called the case "one of the most elaborate insider trading schemes in history." At the core of the scheme, a disgruntled part-time computer graphics worker allegedly went online and found other disgruntled investors of the company in America Online chat rooms. He soon was passing inside information on clients of Goldman Sachs and Credit Suisse First Boston to two other individuals in exchange for a percentage of any profits they earned by acting on it. For 2½ years, this employee passed inside information, communicating almost solely through online chats and instant messages. The part-time computer graphics worker received $170,000 in kickbacks while his partners made $500,000.

Other individuals also became involved as the three defendants who hatched the scheme passed the inside information. More and more individuals became aware of the insider information. For instance, one individual allegedly opened a brokerage account and told his broker, that he had inside information, and the broker then tipped off three of his customers, allowing them to earn more than $2.6 million.

There is a need for a proactive approach when investigating Internet fraud. There is an essential need to establish a central repository for complaints of Internet Fraud. The FBl and the National White Collar Crime Center (NW3C) are addressing this need by cosponsoring the Internet Fraud Complaint Center (IFCC). This partnership will ensure that lnternet fraud is addressed at all levels of law enforcement (local, state and federal). The IFCC is necessary to adequately identify, track, and investigate new fraudulent schemes on the Internet on a national and international level. IFCC personnel will collect analyze, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC will provide a mechanism by which Internet fraud schemes are identified and addressed through a criminal investigative effort. The IFCC will provide analytical support, and aid in the development of a training module to address Internet fraud. The information obtained from the data collected will provide the foundation for the development of a national strategic plan to address Internet fraud. The IFCC will be open and fully operational on May 8, 2000.

Intellectual Property Rights. 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.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

The recent distributed denial of service (DDOS) attacks have garnered a tremendous amount of interest in the public and in the Congress. Because we are actively investigating these attacks, I cannot provide a detailed briefing on the status of our efforts. However, I can provide an overview of our activities to deal with the DDOS threat beginning last year and of our investigative efforts over the last several weeks.

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.

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

The public has downloaded these tools tens of thousands of times from the web site, and has responded by reporting many installations of the DDOS software, thereby preventing their networks from being used in attacks and leading to the opening of criminal investigations both before and after the widely-publicized attacks of the last few weeks. The NIPC's work with private companies has been so well received that the trade group SANS awarded their yearly Security Technology Leadership Award to members of the NIPC's Special Technologies Applications Unit.

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

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

On February 7, 2000, the 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. Several FBI field offices have opened investigations and almost all of our other offices are supporting these cases. 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. 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, SIPC 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.

THE LEGAL LANDSCAPE

To deal with this crime problem, we must look at whether changes to the legal procedures governing investigation and prosecution of cyber crimes are warranted. The problem of Internet crime has grown at such a rapid pace that the laws have not kept up with the technology. The FBI is working with the Department of Justice to propose a legislative package for your review to help keep our laws in step with these advances.

One example of some of the problems law enforcement is facing is the jurisdictional limitation of pen registers and trap-and-trace orders issued by federal district courts. These orders allow only the capturing of tracing information, not the content of communications. Currently, in order to track back a hacking episode in which a single communication is purposely routed through a number of Internet Service Providers that are located in different states, we generally have to get multiple court orders. This is because, under current law, a federal court can order communications carriers only within its district to provide tracing information to law enforcement. As a result of the fact that investigators typically have to apply for numerous court orders to trace a single communication, there is a needless waste of time and resources, and a number of important investigations are either hampered or derailed entirely in those instances where law enforcement gets to a communications carrier after that carrier has already discarded the necessary information. For example, Kevin Mitnick evaded attempts to trace his calls by moving around the country and by using cellular phones, which routed calls through multiple carriers on their way to the final destination. It was impossible to get orders quickly enough in all the jurisdictions to trace the calls.

With regards to additional legal mechanisms needed by law enforcement to help maintain our abilities to obtain usable evidence in an encrypted world, last September the Administration announced a "New Approach to Encryption." This new approach included significant changes to the nation's encryption export policies and, more importantly, 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, the President, on behalf of law enforcement, transmitted to Congress a legislative proposal entitled the "Cyberspace Electronic Security Act of 1999" (CESA). CESA, if enacted would: (1) protect sensitive investigative techniques and industry trade secrets from unnecessary disclosure in litigation or criminal trials involving encrypted evidence; (2) authorize $80 million for the FBI's Technical Support Center (TSC), which will serve as a centralized technical resource for federal, state and local law enforcement in responding to the increased use of encryption in criminal cases; and (3) ensure that law enforcement maintains its ability to access decryption information stored with third parties, while protecting such information from inappropriate release. The enactment of the CESA legislative proposal is supported by the law enforcement community, to include the International Association of Chiefs of Police, the National Sheriffs' Association and the National District Attorneys Association and I strongly encourage its favorable consideration by Congress.

Finally, we should consider whether current sentencing provisions for computer crimes provide an adequate deterrence. Given the degree of harm that can be caused by a virus, intrusion, or a denial of service—in terms of monetary loss to business and consumers, infringement of privacy, or threats to public safety when critical infrastructures are affected—it would be appropriate to consider, as S. 2092 does, whether penalties established years ago remain adequate.

Evaluation of the effectiveness of 18 U.S.C. § 1030 and the tools to enforce it under both current law and under S. 2092

Generally, 18 U.S.C. § 1030 has enabled the FB1 and other law enforcement agencies to investigate and prosecute persons who would use the power of the Internet and computers for criminal purposes. Nonetheless, just as computer crime has evolved and mutated over the years, so too must our laws and procedures evolve to meet the changing nature of these crimes.

One persistent problem is the need under current law to demonstrate at least $5,000 in damage for certain hacking offenses enumerated by 18 U.S.C. § 1030(a)(5). In some of the cases investigated by the FBI, damages in excess of $5,000 on a particular system are difficult to prove. In other cases, the risk of harm to individuals or to the public safety posed by breaking into numerous systems and obtaining root access, with the ability to destroy the confidentiality or accuracy of crucial—perhaps lifesaving information—is very real and very serious even if provable monetary damages never approach the $5,000 mark. In investigations involving the dissemination or importation of a virus or other malicious code, the $5,000 threshold could potentially delay or hinder early intervention by Federal law enforcement.

S. 2092 significantly adjusts the $5,000 threshold impediment and other provisions in the current law by: (1) creating a misdemeanor offense for those cases where damages are below $5,000, while simultaneously adjusting the minimum mandatory sentences under the Sentencing Guidelines; and (2) moving the aggravating factors previously included in the definition of "damage" under 18 U.S.C. § 1030(e)(8) (such as impairment of medical diagnosis, physical injury to any person, threat to public health or safety or damage to national security, national defense or administration of justice computers) to the general sentencing provisions of § 1030(c) (where they will be on par in serious cases with the existing $5,000 threshold requirement and will expose offenders to an enhanced ten-year period of imprisonment up from the current maximum of five years). The critical element here is that the criminal intended to cause damage, not the specific amount of damage he intended to cause.

Another issue involves the alarming number of computer hackers encountered in our investigations who are juveniles. Under current law, Federal authorities are not able to prosecute juveniles for any computer violations of 18 U.S.C. § 1030. S. 2092 would authorize, but not require, the Attorney General to certify for juvenile prosecution in Federal court youthful offenders who commit the more serious felony violations of section § 1030. Recognizing that this change will, over time, result in the prosecution of repeat offenders, S. 2092 also defines the term "conviction" under § 1030 to include prior adjudications of juvenile delinquency for violations of that section.

Similarly, a majority of the States have enacted criminal statutes prohibiting unauthorized computer access analogous to the provisions of section 1030. As State prosecutions for these offenses increase, the likelihood of encountering computer offenders in Federal investigations who have prior State convictions will similarly rise. The Justice Department is studying whether prior state adult convictions for comparable computer crimes justify enhanced penalties for violations of section 1030, just as prior State convictions for drug offenses trigger enhanced penalties for comparable Federal drug violations.

Law enforcement also needs updated tools to investigate, identify, apprehend and successfully prosecute computer offenders. Today's electronic crimes, which occur at the speed of light, cannot be effectively investigated with procedural devices forged in the last millennium during the infancy of the information technology age. Statutes need to be rendered technology neutral so that they can be applied regardless of whether a crime is committed with pen and paper, e-mail, telephone or geosynchronous orbit satellite personal communication devices.

As discussed above, a critical factor in the investigation of computer hacking cases is law enforcement's ability to swiftly identify the source and the direction of a hacker's communications. Like all law enforcement agencies, the FBI relies upon the pen register and trap and trace provisions contained in 18 U.S.C. § 3121 *et seq.* to seek court approval to acquire data identifying non-content information relating to a suspect's communications. Our ability to identify the perpetrators of crimes like computer hacking is directly proportional to our ability to *quickly* acquire the necessary court orders and *quickly* serve them upon one or more service providers in a communications chain. Under current law, however, valuable time is consumed in acquiring individual court orders in the name of each communications company for each newly discerned link in the communications chain even though the legal justification for the disclosure remains unchanged and undiminished. S. 2092 would amend 18 U.S.C. § 3123(a) to authorize Federal courts to issue one nation-wide order, which may then be served upon one or more service providers, thereby substantially reduc-

ing the time necessary to identify the complete pathway of a suspect's communication. Second, S. 2092 makes the statute more technology neutral by, among other things, inserting the terms "or other facility" wherever "telephone" appears. This change codifies Federal court decisions that apply the statute's provisions not merely to traditional telephone, but to an ever expanding array of other, communications facilities. Together, these are important changes that do not alter or lower the showing necessary for the issuance of the court order but which do enhance the order's usefulness to law enforcement.

We support the goal of S. 2092 to strengthen the general deterrence aspects of the Computer Fraud and Abuse Act, and to provide some needed procedural enhancements to help us confront the expanding criminal threat in this dynamic and important part of our national economy while continuing to protect individual privacy interests. The FBI looks forward to working with the Committee on this important legislation.

KEEPING LAW ENFORCEMENT ON THE CUTTING EDGE OF CYBER CRIME

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

We can clearly expect these upward trends to continue. To meet this challenge, we must ensure that we have adequate resources, including both personnel and equipment, both at the NIPC and in FBI field offices. Those personnel need specialized training to be effective. Like many programs, the NIPC computer intrusion program is squeezing the most out of every taxpayer dollar.

At the NIPC, we currently have 101 personnel on board, including 82 FBI employees and 19 detailees from other government agencies. This cadre of investigators, computer scientists, and analysts perform the numerous and complex tasks outlined above, and provide critical coordination and support to field office investigations. As the crime problem grows, we need to make sure that we keep pace by maintaining a full complement of authorized staff, including both FBI personnel and detailees from other agencies and the private sector. Although expert personnel in this area are scarce, it is imperative that our partner agencies participate in the NIPC to enhance our ability to coordinate interagency activities and share information effectively.

We currently have 193 agents in FBI field offices nationwide assigned to investigate computer intrusions (criminal and national security), denial of service, and virus cases, and to work infrastructure protection matters generally (which includes outreach to industry and state and local law enforcement, our Key Asset Initiative, and support to other investigative programs). Additional agents can be called in on investigations as required. In order to maximize investigative resources the FBI has taken the approach of creating regional squads in 16 field offices that have sufficient size to work complex intrusion cases and to assist those field offices without a NIPCI squad. In those field offices without squads, the FBI is building a baseline capability by having one or two agents to work NIPC matters.

In an effort to better use our resources and leverage the expertise of other agencies, we are creating cyber crime task forces in FBI field offices. Last week we unveiled the Pittsburgh High Tech Computer Crimes Task Force, a new task force aimed at fighting cyber crimes. The task force, one of the first in the nation, pools experts from local agencies such as the Pittsburgh police with federal agencies such as the FBI, Secret Service and the Internal Revenue Service into one room to combat the rapid growth of cyber crimes. The task force will use each agency's resources and obtain technical assistance from Carnegie Mellon's Computer Emergency Response Team (CERT).

In addition to putting in place the requisite number of agents, analysts, and computer scientists in the NSC and in FBI field offices, we must fill those positions by recruiting and retaining personnel who have the appropriate technical, analytical, and investigative skills. This includes personnel who can read and analyze complex log files, perform all-source analysis to look for correlations between events or attack signatures and glean indications of a threat, develop technical tools to address the

constantly changing technological environment, and conduct complex network investigations.

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

The technical challenges of fighting crime in this arena are 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.

Developing and deploying state-of-the-art equipment in support of the NIPC's mission is also very important. Conducting a network intrusion or denial-of-service investigation often requires investigative analysis of voluminous amounts of data. For example, one network intrusion case involving an espionage matter currently being investigated has required the analysis of 17.5 Terabytes of data. To place this into perspective, the entire collection of the Library of Congress, if digitized, would comprise only 10 Terabytes. The Yahoo DDOS attack involved approximately 630 Gigabytes of data, which is equvalent to enough printed pages to fill 630 pickup trucks with paper. The NIPC's technical analysis requires high capacity equipment to store, process, analyze, and display data. Again, as the crime problem grows, we must ensure that our technical capacity keeps pace.

Clearly, the FBI needs engineering personnel to develop and deploy sophisticated electronic surveillance capabilities in an increasingly complex and technica] 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.

Moreover, thc power of personal computers in increasing. 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 fill, the CART examiner must review every bit of data and every area of the media to search for evidence.

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), Counterterrorisrn, 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 data interception capabilities, investigators and prosecutors will be denied timely access to valuable evidence that will solve crimes and support the successfull prosecutions of child pornographers, drug traffickers, corrupt officials, persons committing fraud, terrorists, and other criminals.

Finally, 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 telecommnunications 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 transmissions, 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.

It is imperative that the FBI, on behalf of the law enforcement commnunity, enhance its technical capabilities in the area of plaintext access to encrypted evidence.

In order to do this, law enforcement needs Congressional support, both in terms of additional funding and authorizations, for developing, maintaining, and deploying technical capabilities that will provide law enforcement with these urgently needed technical capabilities and meet the public safety challenges posed by the criminal use of encryption. Included in the Administration's "New Approach to Encryption" announcement last September was support for the creation of the FBI's Technical Support Center, which will serve as a centralized technical resource for federal, state and local law enforcement with the necessary technical capabilities to respond to the increased use of encryption in criminal cases. The Technical Support Center is envisioned as an expansion of the FBI's Engineering Research Facility (ERF) to take advantage of ERF's existing institutional and technical expertise in this area. The Administration's "Cyberspace Electronic Security Act of 1999" legislative propossl includes a provision authorizing $80 million over four years for the Technical Support Center. The President's fiscal year 2001 budget includes a $7 million enhancement for this effort.

CONCLUSION

I want to thank thc subcommittees again for giving me the opportunity to testify here today. The cyber crime problem is real, and growing. The NIPC is moving aggressively to meet this challenge by trailing FBI agents and investigators from other agencies on how to investigate computer intrusion cases, equipping them with the latest technology and technical assistance, developing our analytic capabilities and warning mechanisms to head off or mitigate attacks, and closely cooperating with the private sector. We have already had significant successes in the fight. I look forward to working with Congress to ensure that we continue to be able to meet the threat as it evolves and grows. Thank you.

Senator KYL. Mr. Miller and Mr. Pethia will be our next panel, and I will wait until everyone has had a chance to take their seats here. We will operate under the 5-minute rule from now on.

Our next panel will look at some roadblocks to better analysis and sharing of information on cyber vulnerabilities and threats. The first witness is Mr. Rich Pethia, director of the Computer Emergency Response Team Centers at Carnegie Mellon University's Software Engineering Institute in Pittsburgh. These centers have provided a central response and coordination facility for computer incidents since 1988.

Last fall, CERT publicized many warnings about the potential for denial of service attacks, as we witnessed in February. They analyzed the vulnerabilities of some systems to being infected with malicious code and used as third-party attackers. Many people heeded CERT's warnings and took steps to protect their computer networks.

Mr. Pethia, thank you for joining us. We will place your full written statement in the record, and in view of the time we would ask for everyone, both questioning and presenting, to limit remarks to 5 minutes, if you would. Thank you very much.

PANEL CONSISTING OF RICHARD D. PETHIA, DIRECTOR, COMPUTER EMERGENCY RESPONSE TEAM CENTERS, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA; AND HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA, ARLINGTON, VA

STATEMENT OF RICHARD D. PETHIA

Mr. PETHIA. Mr. Chairman and members of the committee, thanks for the opportunity to speak to you on the issue of cyber defense. My perspective comes from the work that we do at the CERT Coordination Center which was established in 1988 and chartered

to respond to security emergencies on the Internet. In total, since then, we have handled well over 24,000 separate security incidents and analyzed more than 1,500 computer vulnerabilities.

The recently published rash of attacks on Internet e-commerce sites reminds us once again of the fragility of many of our sites on the Internet. Managing the risk that comes from an ever-expanding use and dependence on information technology will require an evolving strategy that stays abreast of changes in the technology, changes in the ways we use the technology, and changes in the way people attack us through our systems and networks.

It is also going to require expanded research programs that lead to fundamental advances in computer security, new information technology products with better security mechanisms, a larger number of technical specialists, improved abilities to investigate and prosecute cyber criminals, and increased and ongoing awareness and understanding of cyber security issues. In the short time I have today, I will focus on this last issue, building awareness and understanding.

The overall picture of vulnerability of threat is complex and it requires collection and analysis of information on vulnerabilities in information technology, evolving attack technology, cyber attacks and cyber attackers, and the effectiveness of defensive practices. And using this understanding requires moving this data to technology producers and system operators and convincing them to act on the information.

Today, these tasks are largely being conducted by a loose-knit network of investigative organizations, security response teams, government and private sector research centers, system and network operators, security product and service vendors, and Government agencies chartered to conduct security improvement efforts. The work of these organizations would be facilitated, I think, if some of the following roadblocks were removed.

First of all, the ongoing Federal debate over who is in charge and the advantages or disadvantages of centralized analysis capabilities. I believe that this problem is a distributed problem. We have distributed the technology, we have distributed the use of the technology, we have distributed the management of technology, and we must distribute the solution to this problem as well.

I don't believe it is possible to have a single analysis center that serves the needs of all the various organizations that need help. If you build it, people won't come. Trust relationships are fragile; they build slowly and they cannot be reassigned. It is simply not possible to build an overall, comprehensive picture of activity on the networks. They are too big, they are growing too quickly, and they are literally being reconfigured and reengineered on the fly.

All of the talent that is needed to perform the various kinds of analysis—and people have to come to this from different perspectives—simply cannot be collected in one place. It is much more effective and cost-efficient to distribute the data rather than trying to collect the people.

Second, I don't believe that centralization is necessarily going to be more efficient. Any central organization can only perform analysis tasks at a certain generic high level of activity, and the detailed work that helps people understand how to apply the results of the

analysis still has to happen. We are not going to replace all of these organizations that have operational responsibility. What we need to do is not focus on how to pull data together, but focus on how to push it out to all the people who must use it.

The second obstacle, I believe, is that we have been talking about, and the Federal Government has been talking about and studying this problem for years, but there hasn't been a significant increase in funding over the years to deal with the problem. Using my own organization as an example, since 1988 our budget has increased by a factor of 5, but yet the workload has increased by a factor of 80.

I don't know of any other organization that is dealing with this security problem who hasn't had the same experience. Every organization out there today is strained because the problem is effectively doubling every year and we simply can't keep up with the problem. Progress will come when analysis centers are funded, when information sharing infrastructures are established, and when we begin to move this data out to the people who need to use it.

Another issue has already been discussed this morning: lack of protection for sensitive and company proprietary data. Information sharing between the private sector and the Federal Government must receive protection from FOIA and other forms of mandatory disclosure not just for trade secrets and other kinds of company proprietary information, but to move information assurance form the ad hoc art that it is today to a real engineering discipline.

We need a detailed understanding of organizations' systems, their policies, their practices, the kinds of information that would make an organization vulnerable. This has to come through Federal organizations as well as federally-funded research programs and that information has to be protected.

Finally, the last thing that I think is central to this, is a better understanding of threats. Today, we are literally awash in a sea of information about vulnerability. We know plenty about the vulnerability in our technologies and in our infrastructures, but we have little real awareness and understanding of the real threats.

Senior executives in Government and industry are going to continue to resist investment in improving information assurance until they have some hard data that convinces them that there are real criminals, real terrorists, real people who are out there to do damage. Incidents like the attacks against e-commerce sites will have an effect, but that effect will be short term; it won't last for more than a few more months.

We seem to deal with crisis situations when they come up, but what we really need to understand—and we need help from the investigative and the intelligence community to do this—is to get better information about the threat that we are all facing and what kinds of real damage might be done. We understand the vulnerability. In the absence of a smoking gun, I think it is unlikely that many organizations will have the motivation to invest in and improve cyber defense.

Thank you.

[The prepared statement of Mr. Pethia follows:]

PREPARED STATEMENT OF RICHARD D. PETHIA

INTRODUCTION

Mr. Chairman and Members of the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information:

My name is Rich Pethia. I am the director of the CERT® Centers, which include the CERT® Coordination Center and the CERT Analysis Center. The centers are part of the Software Engineering Institute (SEI) at Carnegie Mellon University. Thank you for the opportunity to speak to you on the issue of cyber defense. Today I will describe a number of issues that have impact on security on the Internet and outline some of the steps I believe are needed to effectively manage the increasing risk of damage from cyber attacks.

My perspective comes from the work we do at the CERT Centers. The CERT® Coordination Center (CERT/CC) was established in 1988, after an Internet "worm" stopped 10 percent of the computers connected to the Internet. This program—the first Internet security incident to make headline news—was the wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was chartered to respond to security emergencies on the Internet and to work with both technology producers and technology users to facilitate response to emerging security problems. In the first full year of operation, 1989, The CERT/CC responded to 132 computer security incidents. In 1999, the staff responded to more than 8,000 incidents. In total, the CERT/CC staff has handled well over 24,000 incidents and analyzed more than 1,500 computer vulnerabilities. More details about our work are attached to the end of this testimony (see *Meet the CERT Coordination Center*).

The recently established CERT® Analysis Center (CERT/AC) addresses the threat posed by rapidly evolving, technologically advanced forms of cyber attacks. Working with sponsors and associates, the CERT Analysis Center collects and analyzes information assurance data to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. The CERT Analysis Center builds upon the work of the CERT Coordination Center. The CERT Analysis Center extends current incident response capabilities by developing and transitioning protective measures and mitigation strategies to defend against advanced forms of attack before they are launched. Additionally, it provides the public and private sectors with opportunities for much-needed collaboration and information sharing to improve cyber attack defenses.

AN EVER-CHANGING PROBLEM

The recently publicized rash of attacks on Internet e-commerce sites reminds us once again of the fragility of many sites on the Internet and of our ongoing need to improve our ability to assure the integrity, confidentiality, and availability of our data and systems operations. While it is important to react to crisis situations when they occur, it is just as important to recognize that cyber defense is a long-term problem. The Internet and other forms of communication systems will continue to grow and interconnect. More and more people and organizations will conduct business and become otherwise dependent on these networks. More and more of these organizations and individuals will lack the detailed technical knowledge and skill that is required to effectively protect systems today. More and more attackers will look for ways to take advantage of the assets of others or to cause disruption and damage for personal or political gain. The network and computer technology will evolve and the attack technology will evolve along with it. Many information assurance solutions that work today will not work tomorrow.

Managing the risks that come from this expanded use and dependence on information technology requires an evolving strategy that stays abreast of changes in technology, changes in the ways we use the technology, and changes in the way people attack us through our systems and networks. The strategy must also recognize that effective risk management in any network like the Internet is unlikely to come from any central authority, but can only be accomplished through the right decisions and actions being made at the end points: the organizations and individuals that build and use our interconnected information infrastructures. Consider this:

- We have distributed the development of the technology—today's networks are made up of thousands of products from hundreds of vendors.
- We have distributed the management of the technology—management of information technology in today's organizations is most likely distributed, and the trend toward increased collaborations and mergers will make that more likely in the future.

• We have distributed the use of the technology—the average computer user today has little in-depth technical skill and is properly focused on "getting the job done" rather than learning the nuances and idiosyncrasies of the technology.
• We must distribute the solution to the information assurance problem as well—the technology producers, organization and systems managers, and systems users are the only ones that can implement effective risk management programs.

In the long run, effective cyber defense will require:

• expanded research programs that lead to fundamental advances in computer security;
• new information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users;
• a larger number of technical specialists who have the skills needed to secure large, complex systems;
• improved abilities to investigate and prosecute cyber criminals; and
• increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space.

With the short time I have with you today, I will focus on removing barriers to the last of these: building an ongoing awareness and understanding of cyber-security issues.

BUILDING AWARENESS AND UNDERSTANDING

Information technology is evolving at an ever-increasing rate with thousands of new software products entering the market each month. Increasingly, cyber security depends not just on the security characteristics and vulnerabilities of basic networking and operating system software, but also on the characteristics and vulnerabilities of software used to implement large, distributed applications (e.g., the World Wide Web). In addition, attack technology is now being developed in an open source environment where a community of interest is evolving this technology at a rapid pace. Several significant new forms of attack have appeared in just the past year (for example, the Melissa virus, which exploits the widespread use of electronic mail to spread at network speeds, and distributed denial-of-service tools that harness the power of thousands of vulnerable systems to launch devastating attacks on major Internet sites). It is likely that attack technology will continue to evolve in this "public" forum and that the evolution will accelerate to match the pace of change in information technology. Once developed, this attack technology can be picked up and used by actors with significant resources to hone and advance the technology, making it a much more serious threat to national security and the effective operation of government and business.

The overall picture of vulnerability and threat is complex, but it must be understood to develop effective cyber-defense strategies. Building this understanding requires:

• Collection and analysis of information on the security characteristics and vulnerabilities of information technology;
• Collection and analysis of information on evolving attack technology;
• Collection and analysis of information on cyber attacks;
• Collection and analysis of information on cyber attackers; and
• Collection and analysis of information on the effectiveness of defensive practices and technologies.

Using this understanding to develop effective defense strategies requires:

• Providing technology producers and the rapidly growing community of system operators with information from the analysis activities; and
• Convincing this community to act on this information to reduce serious vulnerabilities and implement effective security controls.

The tasks described above are currently being conducted by a loose-knit network of cooperating organizations. Each organization focuses on its area of expertise and the needs of its customers or constituents. Each organization shares as much information as it can with others. Many varied organizations participate in this network, including federal, state, and local investigative organizations, security incident response teams, government labs and federally-funded research and development centers, security researchers in universities and industry, technology producing organizations, security product and service vendors, system and network operators, and government agencies chartered to conduct security improvement efforts. The work of these organizations would be facilitated if the roadblocks described below were removed.

The federal debate over who's in charge.—The ongoing federal debate over who's in charge and whether or not the grand analysis center in the sky should be established is only detracting from the real work that is going on in the qualified organizations listed above. The Department of Defense must conduct data collection and analysis activities to operate and protect its networks. The FBI and NIPC must conduct data collection and analysis activities to carry out their missions of criminal investigation and infrastructure defense. GSA and NIST must conduct data collection and analysis activities to carry out their missions of dealing with incidents and improving security in the civilian agencies. University and industry researchers are among the best resources available to understand the evolution of information technology, attack technology and the interplay between them. The other organizations listed above must conduct data collection and analysis activities to meet the needs of their customers and sponsors. Attempts to replace these activities with one central data collection and analysis activity are misguided and seemingly miss the following realities.

- If you build it, they won't come—Sharing of sensitive security information is dependent on the trust relationship established between the information sender and receiver. These relationships are fragile, often take years to establish, and cannot be replaced by changing mandates or reassigning responsibilities.
- It is not possible to build an overall, comprehensive picture of activity on the networks—In spite of the strong desire to "see it all" so we can "understand it all," it is simply not possible to build a comprehensive view of activity on the networks. They are too big; they are growing too quickly; they lack the needed sensors; and they are literally being reconfigured and re-engineered on the fly. The challenge is not to pull all the data together, but to ensure that the right data is at the right place at the right time to allow local decision-makers to take effective action.
- All the talent needed to perform the analysis cannot be collected in one place—The detailed analysis work that must be done requires a combination of talents and skills and the best people that we can find. Organizations are not willing to give up their best people to other organizations, and the people are not willing move. It is much more effective and efficient to move the data than to move the people. What is needed is an information-sharing network where data can be shared among organizations and analysis conducted at different sites for different reasons. The challenge is not to pull all data together, but to push it out to meet the varying needs of the various audiences.
- Centralization is not more efficient—Any central organization, unfamiliar with the operational needs of any particular network operator, technology developer, or researcher, will only be able to perform generic analysis tasks that yield high-level results. The detailed work must still be done to develop the detailed strategies and plans needed to build an effective cyber defense. Centralization is more likely to increase costs rather than decrease them. What is needed is increased collaboration among all players able to contribute to and draw from a growing body of data and knowledge.

Inadequate resources for the work that must be done.—The federal government has studied and debated the cyber-security problem for years. The newest flurry of activity began with the Presidential Commission on Critical Infrastructure Protection in 1996 and has led to the establishment of the National Infrastructure Protection Center and the creation of the National Plan for Information System Protection. However, many of the views being discussed and debated today are echoes of earlier studies and conclusions. The 1989 DARPA-funded study, *Computers at Risk**, reached many of the same conclusions and recommended many of the same actions as the more recent studies. What has been missing is action and funding to take the steps needed to deal with this problem effectively. In spite of the nearly exponential growth of security incidents and security vulnerabilities over the last ten years, there has been little increase in budget to deal with these problems. Analysis centers must be resourced, information-sharing infrastructures must be established, and transition activities that move needed information and security solutions their eventual users must be staffed. We will make progress when we invest in making progress.

Lack of protection for sensitive and company proprietary data.—Information sharing between the private sector and the federal government is impeded by the lack of protection from FOIA and other forms of disclosure. Organizations that are the victims of cyber attacks can contribute greatly to the understanding of cyber defense by providing detailed information regarding the security incidents they have suf-

---

**Computers at Risk: Safe Computing in the Information Age,* National Research Council. Washington, D.C.: National Academy Press, 1991.

fered: losses, methods of attack, configurations of systems that were successfully attacked, processes used by the organization that were vulnerable, etc. Much of this information is extremely sensitive and could be used to damage the corporation if it became public. In addition, corporations often have more to lose from damaged reputations than from the attacks themselves. These organizations will not share security incident or loss information unless they have a high degree of confidence that this information will be protected from public disclosure. The federal government must take steps to protect the sensitive data as a precursor to information sharing. Only then will it be possible to form the trust relationships and begin data-sharing activities.

Lack of information on threats.—Any effective risk management strategy requires an understanding of three things:

1. The value of the assets that must be protected and the consequences of loss of confidentiality or operational capability
2. The vulnerabilities that could be exploited to bring about the losses
3. The threats that exist—the actors that would exploit the vulnerabilities and some indication of the probability that they would do so

Today we are awash in information regarding vulnerabilities in our technologies and our networked systems. Computer security incident response teams warn their constituents of vulnerabilities that are being exploited. Internet news groups routinely publish descriptions of vulnerabilities and methods to exploit them. Technology vendors alert their customers to vulnerabilities in their products and provide software upgrades to correct them. Conferences and training courses abound that focus on corrections to vulnerabilities.

At the same time, system and network operators are becoming increasingly aware of the value of their information assets and of their growing dependence on the Internet and other communications infrastructures. The current emphasis on electronic commerce and use of the Internet as a powerful marketing and sales tool is sure to accelerate this understanding.

With all this focus on value and vulnerability, why are so many organizations taking so little action to improve their cyber-security? Because they have little hard data that convinces them that there are real threats to their operations. We all know that we are vulnerable to many things. Our cars are vulnerable to certain forms of attack. Our homes and places of business are vulnerable to certain forms of attack. As individuals, we are vulnerable to certain forms of attack yet we are not all driven to distraction by this sea of vulnerability. We first focus not on vulnerability but on threat. We act to correct vulnerabilities when we believe there is a significant probability that someone will take advantage of them. The same is true in cyber space. Operational managers know that they cannot afford to eliminate every vulnerability in their operations. They need data to help them understand which ones are most critical; and which ones are likely to be exploited.

Our law enforcement and intelligence organizations must find ways to release threat data to the operational mangers of information infrastructures to motivate these managers to take action and to help them understand how to set their priorities. In the absence of a smoking gun, it is unlikely that many organizations will have the motivation to invest in improved cyber defense.

Job title

Manager, Networked Systems Survivability (NSS) Program

Key responsibilities

Provide strategic direction for the Networked Systems Survivability Program and its CERT® Coordination Center activity.

Professional background

Mr. Pethia has managed the NSS Program since 1995. The NSS program improves both practices and understanding of security and survivability issues relating to critical information infrastructures. The NSS program draws heavily on the security incident and vulnerability data gained from its CERT® Coordination Center (CERT/CC) to further applied research and development efforts. The SEI has operated the CERT/CC since 1988, and has provided a central response and coordination facility for global information security incident response and countermeasures for threats and vulnerabilities.

Prior to joining the SEI, Mr. Pethia was director of engineering at Decision Data Computer Company, a computer system manufacturer in Philadelphia, Pennsylvania. There he was responsible for engineering functions and resource management in support of new product development.

Mr. Pethia also was manager of operating systems development for Modular Computer Corporation in Fort Lauderdale, Florida. While there he lead development efforts focused on real-time operating systems, networks, and other system software in the application areas of industrial automation, process control, data acquisition, and telecommunications.

Contact information

Electronic mail address: *rdp@sei.cmu.edu*
Phone: (412) 268-7739
Fax: (412) 268-6989
Room 4108

MEET THE CERT® COORDINATION CENTER

OVERVIEW

The CERT Coordination Center (CERT/CC) is located at the Software Engineering Institute (SEI), a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Internet Worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. Since then, the CERT/CC has helped to establish other response teams and our incident handling practices have been adopted by more than 80 response teams around the world.

While we continue to respond to security incidents and analyze product vulnerabilities, our role has expanded over the years. Each year, commerce, government, and individuals grow increasingly dependent on networked systems. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, the CERT/CC is now part of the larger SEI Networked Systems Survivability Program, whose primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks (“survivability”).

To accomplish our goals, we focus our efforts on the following areas of work: survivable network management, survivable network technology, incident response, incident and vulnerability analysis, knowledgebase development, and courses and seminars.

We are also committed to increasing awareness of security issues and helping organizations improve the security of their systems. Therefore, we disseminate information through several channels.

AREAS OF WORK

Survivable network management

Our survivable network management effort focuses on publishing security improvement practices, developing a self-directed method for organizations to improve the security of their network computing systems, and defining an adaptive security improvement process.

Security improvement practices provide concrete, practical guidance that will help organizations improve the security of their networked computer systems. These practices are published as security improvement modules and focus on best practices that address important problems in network security. We have published seven modules, incorporating more than 80 recommended practices and technology-specific implementations. A complete list of the modules, practices, and implementations can be found on the CERT/CC Web site at: *http://www.cert.org/security-improvement/*

Our self-directed security evaluation method will give organizations a comprehensive, repeatable technique that can be used to identify risk in their networked systems and keep up with changes over time. The method takes into consideration assets, threats, and vulnerabilities (both organizationally and technologically) so that the organization gains a comprehensive view of the state of its systems’ security.

Additionally, the adaptive security management process, that we have under development, builds on and incorporates our work on security practices and self-directed security evaluations. The adaptive process presents a structure that an organization can use to develop and execute a plan for continuously improving the security of its networked systems.

Survivable network technology

In the area of survivable network technology, we are concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems such as the Internet. Therefore, new approaches to system security must be developed. They include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. This work draws on the vast collection of incident data collected by the CERT/CC. For introductory information, technical reports, and more, see: *http://www.cert.org/research*

Incident response

We provide assistance to computer system administrators in the Internet community who report security problems. When a security breach occurs, we help the administrators of the affected sites to identify and correct the vulnerabilities that allowed the incident to occur. We will also coordinate the response with other sites affected by the same incident. When a site specifically requests, we will facilitate communication with law enforcement agencies.

Since our inception in 1988, we have received more than 260,000 email messages and 17,600 hotline calls reporting computer security incidents or requesting information. We have handled more than 24,300 computer security incidents and received more than 1,500 vulnerability reports.

The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. Therefore, the CERT/CC staff regularly works with sites to help them form incident response teams and provides guidance to newly formed teams.

FedCIRC.—We are responsible for the day-to-day operations of FedCIRC, the Federal Computer Incident Response Capability, an organization that provides incident response and other security-related services to Federal civilian agencies. FedCIRC is managed by the General Services Administration (GSA).

More information about FedCIRC is available from *http://www.fedcirc.gov/*. Federal agencies can contact FedCIRC by sending email to *fedcirc-info@fedcirc.gov* or by calling the FedCIRC Management Center at (202) 708–5060. To report an incident, affected sites should send email to *fedcirc@fedcirc.gov* or phone the FedCIRC hotline at (888) 282–0870.

Incident and vulnerability analysis

Our ongoing computer security incident response activities help the Internet community to deal with its immediate problems while allowing us to understand the scope and nature of the problems and of the community's needs. Our understanding of current security problems and potential solutions comes from first-hand experience with compromised sites on the Internet and subsequent analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities.

The CERT/CC has become a major reporting center for incidents and vulnerabilities because we have an established reputation for discretion and objectivity. Organizations trust us with sensitive information about security compromises and network vulnerabilities because we have proven our ability to keep their identities and other sensitive information confidential. Our connection with the Software Engineering Institute and Carnegie Mellon University contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of the community's trust, we are able to obtain a broad view of incident and vulnerability trends and characteristics.

When we receive a vulnerability report, our vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

To achieve long-term benefit from vulnerability analysis, we have begun to identify the underlying software engineering and system administration practices that lead to vulnerabilities and, conversely, practices that prevent vulnerabilities. We will broadly disseminate this information to practitioners and consumers and influence educators to include it in courses for future software engineers and system administrators. Only when software is developed and installed using defensive prac-

tices will there be a decrease in the expensive, and often haphazard, reactive use of patches and workarounds.

Knowledgebase development

We are developing a knowledgebase that will help to capture and effectively use information related to network survivability and security. The work includes developing processes and tools to support the increasing complexity of handling incidents, analyzing vulnerabilities, and managing the volume of information that is essential to the CERT/CC mission. We are forming collaborative relationships with other organizations to support this work.

Education and training

We offer public training courses for technical staff and managers of computer security incident response teams (CSIRTs) as well as for system administrators and other technical personnel interested in learning more about network security. In addition, several CERT/CC staff members teach courses in the Information Security Management specialization of the Master of Information Systems Management program in the H. J. Heinz III School of Public Policy and Management at Carnegie Mellon University. For more information, see:
http://www.cert org/training/index.html

INFORMATION DISSEMINATION

To increase awareness of security issues and help organizations improve the security of their systems, we collect and disseminate information through multiple channels:

- telephone and email; hotline: (412) 268–7090; email: *cert@cert.org*; mailing list: *cert-advisory-request@cert.org*
- USENET newsgroup: comp.security.announce
- World Wide Web: *http://www.cert.org*
- anonymous FTP: *ftp://ftp.cert.org/pub/*

Since beginning operation in 1988, we have handled more than 17,600 hotline calls and 260,600 mail messages. We have published 290 security alerts (advisories, vendor-initiated bulletins*, incident notes, vulnerability notes, and CERT summaries).

Publications

Advisories.—CERT/CC advisories address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, fixes or workarounds, and vendor information. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and the existence of a software patch or workaround. On the day of release, we send advisories to a mailing list, post them to the USENET newsgroup comp.security.announce and make them available on the CERT Web site at *http://www.cert.org/advisories/*.

CERT Summaries.—We publish the CERT Summary as part of our ongoing efforts to disseminate timely information about Internet security issues. The summary is typically published four to six times a year. The primary purpose of the summary is to call attention to the types of attacks currently being reported to the CERT/CC. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks. Summaries are distributed in the same way as advisories.

Incident Notes and Vulnerability Notes.—We publish two web documents, Incident Notes and Vulnerability Notes, as an informal means for giving the Internet community timely information relating to the security of its sites. Incident Notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability Notes describe weaknesses in Internet-related systems that could be exploited but that do not meet the criteria for advisories.

Security Improvement Modules.—Security Improvement Modules address an important but narrowly defined problem in network security. They provide concrete, practical guidance that will help organizations improve the security of their network computer systems. The modules are available on the CERT Web site at *http://www.cert.org/security-improvement/*. We have published, in Web form only, technology-specific implementation details for the modules.

Other Security Information.—We capture lessons learned from incident handling and vulnerability analysis and make them available to users of the Internet through

* Publication of vendor-initiated bulletins was discontinued in 1999.

a web site archive of security information and products. These include answers to frequently asked questions, a security checklist, "tech tips" for system administrators, research and technical reports, and a handbook for new computer security incident response teams (CSIRTs).

ADVOCACY AND OTHER INTERACTIONS WITH THE COMMUNITY

The CERT/CC has the opportunity to advocate high-level changes that improve Internet security and network survivability. Additionally, CERT/CC staff members are invited to give presentations at conferences, workshops, and meetings. These activities enhance the understanding of Internet security and related issues.

Forum of Incident Response and Security Teams (FIRST).—FIRST is a coalition of individual response teams around the world. Each response team builds trust within its constituent community by establishing contacts and working relationships with members of that community.

These relationships enable response teams to be sensitive to the distinct needs, technologies, and policies of their constituents. FIRST members collaborate on incidents that cross boundaries, and they cross-post alerts and advisories on problems relevant to their constituents.

The CERT/CC was a founding member of FIRST, and staff members continue to be active participants in FIRST. A current list of FIRST members is available from *www.first.org/team-info/*. More than 80 teams belonged to FIRST, and membership applications for additional teams are pending.

Internet Engineering Task Force

Members of our staff influence the definition of Internet protocols through participation in the Internet Engineering Task Force (IETF); a member of our staff sits on the Security Area Advisory Group to ensure that the CERT/CC perspective is brought to bear on all new standards activities.

Vendor relations

We work closely with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Staff members have worked to influence the vendors to improve the basic, as shipped, security within their products and to include security topics in their standard customer training courses. We interact with more than 100 vendors, as well as developers of freely available software such as sendmail and BIND.

Vendors often provide information to the CERT/CC for inclusion in advisories.

External events

CERT/CC staff members are regularly invited to give presentations at conferences, workshops, and meetings. We have found this to be an excellent tool to educate attendees in the area of network information system security and incident response.

Media relations

Internet security issues increasingly draw the attention of the media. The headlines, occasionally sensational, report only a small fraction of the events that are reported to the CERT/CC. Even so, accurate reporting on security issues can raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, the increased visibility of security issues may lead consumers to demand increased security in the computer systems and network services they buy.

In the course of a year, the CERT/CC is referred to in major U.S. newspapers and in a variety of other publications, from the Chronicle of Higher Education to IEEE Computer. Our staff gives interviews to a selected number of reporters, under the guidance of the SEI public affairs manager.

In 1999, the CERT/CC has been covered in radio, television, print, and online media around the world, including US News and World Report, USA Today, the San Jose Mercury News, The New York Times, The Wall Street Journal, The Washington Post, the Chicago Sun-Times, The Toronto Star, the Ottowa Citizen, Agence Eqrance Presse, Deutsche Presse-Agentur, the Xinhua News Agency, MSNBC, Ziff-Davis ZDNET, BBC London, National Public Radio, ABC, CNN, NBC, and more.

APPENDIX A: THE CERT/CC CHARTER

The CERT/CC is chartered to work with the Internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents. In particular, our mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

APPENDIX B: THE CERT/CC AND THE INTERNET COMMUNITY

The CERT/CC operates in an environment in which intruders form a well-connected community and use network services to quickly distribute information on how to maliciously exploit vulnerabilities in systems. Intruders dedicate time to developing programs that exploit vulnerabilities and to sharing information. They have their own publications, and they regularly hold conferences that deal specifically with tools and techniques for defeating security measures in networked computer systems.

In contrast, the legitimate, often overworked, system administrators on the network often find it difficult to take the time and energy from their normal activities to stay current with security and vulnerability information, much less design patches, workarounds (mitigation techniques), tools, policies, and procedures to protect the computer systems they administer.

In helping the legitimate Internet community work together, we face policy and management issues that are perhaps even more difficult than the technical issues. For example, one challenge we routinely face concerns the dissemination of information about security vulnerabilities. Our experience suggests that the best way to help members of the network community to improve the security of their systems is to work with a group of technology producers and vendors to develop workarounds and repairs for security vulnerabilities disclosed to the CERT/CC. To this end, in the absence of a major threat, we do not publicly disclose vulnerabilities until a repair or workaround has been developed.

Last updated February 16, 2000

Senator KYL. Well, that is sobering and we will get to some questions here in just a bit.

Our next witness is Mr. Harris Miller, president of the Information Technology Association of America. ITAA is the oldest and largest information technology trade association, representing 26,000 software services, Internet, telecommunications, electronic commerce, and systems integration companies. Mr. Miller is also president of the World Information Technology and Services Alliance, representing 41 high-tech trade groups around the world.

Thank you, Mr. Miller, for joining us. We will place your full written statement in the record as well, and invite you to make a summary statement at this time.

STATEMENT OF HARRIS N. MILLER

Mr. MILLER. Thank you, Senator Kyl and Senator Feinstein, and my commendations to you for holding this hearing. The title of this hearing, "Cyber Attacks" "Removing Roadblocks to Investigation and Information Sharing," itself is very encouraging because the roadblocks and the potholes are real. But I continue to believe that the road to common ground and information sharing can be navigated and we can achieve information sharing, with some qualifications.

Assessing the ultimate InfoSec responsibility and roles for the Government agencies and for the private sector is really very simple. Our new information-based assets both domestically and globally must be protected and preserved. We at ITAA have been working for several years to execute a multifaceted plan designed to improve cooperation on information security.

However, it is important to point out that it is not just the IT industry, it is not just government, it is everyone. We must work across industry, we must work industry with government. To think of it metaphorically, if the Public Health Service put out a warning and only a certain percentage of the population got that warning to cover their mouths when they cough, two bad things would happen. No. 1, all the people who didn't get that warning would all cough over each other and they would get sick, plus they would cough all over the people who did cover their mouths and they would get sick, too.

The uniqueness of the Internet that it is so open is its blessing and its curse. So solving the problem uniquely in the IT industry or within the banking industry or within government will not solve the problem. We must all work together.

We have a unique role as an association because we have been appointed as the sector coordinator for the information and communications sector by the Department of Commerce, along with the Telecommunications Industry Association and the U.S. Telephone Association. We are exploring all aspects of this problem. Our overall plan includes awareness, education, training, developing best practices, research and development, international coordination, and the major topic of today's hearing, information sharing.

It is important to note that in this information sharing focus, difficulties exist sharing information not just between industry and government, but, Senators, sharing information within the industry and across industries. This is not a slam dunk on any front, and so the committee should not think that the only challenge is getting cooperation between industry and government. Getting information sharing even within industry itself is a major challenge.

Why are companies reluctant to share information? You have already heard many of them come forward in the earlier questions. The possibility of negative publicity; the loss of confidence of customers, of shareholders; the possible exposure of major vulnerabilities—all these are reasons. Customers are fearful of revealing trade secrets. They fear that information that does go to the Government, notwithstanding the well-intentioned reassurances of Director Freeh, will, in fact, end up in the public news.

So whether, again, we are talking about information sharing within industry, across industries, or between industry and government, the concern about trust—and I keep coming back to that word because I think it is so key, Senator—is something that we must overcome.

We also, of course, must be concerned, and companies are very concerned about protecting customers' privacy. We believe security and privacy are necessarily interlinked, but industry is concerned that if they share information, they may run into situations where inadvertently individual privacy is breached and they run into the bad side of that whole issue.

How do we deal with this challenge? How do we work on developing the trust? Well, in terms of the overall approach, Senator, our simple comment at the top is we must find industry leadership. Industry controls over 90 percent of the assets which you were discussing, and you and Senator Schumer and Senator Feinstein mentioned in your opening comments that industry leadership is key. Regulation is not the answer.

So what do these industry leadership structures look like? Well, we have been working very closely with the Department of Justice, the National Security Council, the NIPC, the Department of Commerce, the Critical Information Assurance Office and the whole melange of agencies within the Government to increase trust and communication.

For example, we are holding a major meeting between many of our member companies and Attorney General Janet Reno next week in California, followed by a meeting here on the East Coast in May, to increase the communication and to discuss how to increase the trust. As another example, we have brought FBI agents forward through their InfoGuard program to meet with many of our local associations to make sure that they can help build the trust and communication.

We also believe that the issues that were raised before, about the Freedom of Information Act, have to be addressed because that could become an obstacle. Another issue we must face is developing trust internationally. As Senator Schumer and others discussed, that is very important, and therefore we are organizing a global information security summit this fall which will be modeled on the Partnership for Critical Infrastructure Protection which is existing domestically to make sure that industry shares information across industries, not just again between industry and Government.

We also believe that the International Information and Coordination Center that Senator Bennett referred to should be maintained for a period of time to determine whether it can play some role in solving information-sharing and trust.

Another issue we are focusing on is young people, which Senator Schumer brought up in his questions. We are in a collaborative partnership with the Department of Justice in what is called a cyber citizen partnership to teach ethics to young people. They have all the technology skills. What they frequently don't have is the basic behavioral rules of the road.

We also believe that there is a need for more money for research and development, and support for the initiative coming out of the Administration for an institute for information infrastructure protection. And another funding source that Congress should look at is more money for training. The problems that Director Freeh outlined in terms of a shortage of people within the Government to do this kind of analysis and forensic exercises—a similar problem exists in the private sector. To put it simply, Senator, we do not have enough skilled people in the IT industry generally, and we certainly don't have enough people with the overall skills to be specialists in information security.

In conclusion, we at ITAA face daunting job of convincing the IT industry and other industries to both work with each other and to work with the Federal Government even under the best of cir-

cumstances. So we must do more to build the trust and the confidence. We must increase the communication. We must work closely with each other and industry and with law enforcement and the national security community, but we must do it in an open and frank dialog where information is shared both ways.

We believe we have made progress over the last 3 years in this dialog. We believe a lot more progress must be made, but we must not underestimate the challenge that lies before us.

Thank you very much.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF HARRIS N. MILLER

INTRODUCTION

Chairman Kyl and Members of this Senate Subcommittee, thank you for inviting me here to testify today on Information Security and Information Sharing. My name is Harris N. Miller, and as President of the largest information technology trade association, the Information Technology Association of America, I am proud that ITAA has emerged as the leading association on the issue of information security. ITAA represents over 26,000 direct and affiliate members who have a vested economic interest in protecting our nation's information security needs since almost 90 percent of the world's information infrastructure, including the Internet, is run by industry. I am also President of the World Information Technology and Services Alliance (WITSA) an association of 41 global IT organizations, so I also have experience in the topic from a global perspective.

The title of this hearing, "Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing," is encouraging. I commend this Subcommittee for holding this hearing and recognizing that in order for industry and government to work together to combat security threats, there are some obstacles, not insurmountable but real, that must be overcome. I continue to believe that though the road to common ground on information sharing contains potholes and detours, it is still navigable.

Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than $1.8 trillion, and over 8 percent of US GDP, according to Digital Planet, a report released by WITSA. Further, a recent US Department of Commerce report indicated that an incredible 35 percent of the nation's real economic growth from 1995 to 1998 came from IT producers. Chairman Alan Greenspan of the US Federal Reserve Board recently credited large investments in high-tech products for the dramatic boost in the nation's productivity. Even previously skeptical economists now concede that IT-driven productivity increases have enabled our country to have what they said we could not have: high growth, low unemployment, low inflation, growth in real wages.

If IT is the engine behind this growth, the Internet and E-commerce are the rocket fuel. Forrester, a respected market research firm, forecasts that the U.S. business-to-business marketplace is worth $290 billion this year and will grow to $2.7 trillion by 2004. The Internet is rewriting economic history.

THE RISE OF "INFOSEC" AS A POLICY ISSUE

Along with the blessings of this new prosperity comes a challenge—new vulnerabilities exhibited by this evolving infrastructure. If we are to continue building our New Economy on this digital foundation, we must meet the security and policy challenges that it poses:

- Stakeholders must be able to trust that the Internet is a safe and secure environment;
- Industry owns and operates most of this infrastructure and, therefore, is its natural steward for safety and security issues;
- Government and industry share an interest in the health and growth of the Internet and E-commerce and must find common ground on which to coordinate on critical information infrastructure protection issues;
- "Cyberethics" must become a regular and understandable part of the Internet lexicon. Ethical on-line behavior must be taught at home, in school and in the workplace. Safe and efficient on-line business operations demand the investment by schools, community groups, IT and non-IT companies and organizations. It is everyone's responsibility to become part of a deterrence solution, working together to establish and embrace a reasonable set of information security practices and procedures;

• Because the Internet is a global medium, which means national boundaries are transparent, information security is an issue that must be pursued on a global basis. The nature of the cybercrime threat is dynamic; information security requires on-going commitment, attention, and cooperation of industry and law enforcement worldwide.

Assessing the ultimate InfoSec responsibility and roles for government agencies and the private sector is really very simple: our new information-based assets must be protected and preserved.

INDUSTRY PLAN FOR CYBER SECURITY

ITAA and its members have been working to execute a multi-faceted plan designed to improve U.S. cooperation on issues of information security. However, Mr. Chairman, we would all be remiss if we believed it was just the IT industry that must cooperate within its own industry—we must work cross industry, and industry with government. Protecting our infrastructure is a collective responsibility, not just the IT community's role.

We are working on multiple fronts to improve the current mechanisms for combating threats and responding to attacks through our role as Sector Coordinator for the Information and Communications sector, appointed by the U.S. Department of Commerce. Through ITAA's InfoSec Committee, our member companies also are exploring joint research and development activities, international issues, and security workforce needs. Elements of the plan include Awareness, Education, Training, Best Practices, Research and Development, International Coordination, and Information Sharing.

Awareness: ITAA and its member companies are raising awareness of the issue within the IT industry and through partnership relationships with other vertical industries, including finance, telecommunications, energy, transportation, and health services. We are developing regional events, conferences, seminars and surveys to educate all of these industries on the importance of addressing information security. An awareness raising campaign targeting the IT industry and vertical industries dependent on information such the financial sector, insurance, electricity, transportation and telecommunications is being overlaid with a targeted community effort directed at CEOs, end users and independent auditors. The goal of the awareness campaign is to educate the audiences on the importance of protecting a company's infrastructure, and instructing on steps they can take to accomplish this. The message is that information security must become a top tier priority for businesses and individuals.

Education: In an effort to take a longer-range approach to the development of appropriate conduct on the Internet, the Department of Justice and the Information Technology Association of America have formed the *Cybercitizen Partnership*. The Partnership is a public/private sector venture formed to create awareness, in children, of appropriate on-line conduct. This effort extends beyond the traditional concerns for children's safety on the Internet, a protective strategy and focuses on developing an understanding of the ethical behavior and responsibilities that accompany use of this new and exciting medium. The Partnership will develop focused messages, curriculum guides and parental information materials aimed at instilling a knowledge and understanding of appropriate behavior on-line. Ultimately, a long range, ongoing effort to insure proper behavior is the best defense against the growing number of reported incidents of computer crime.

Training: ITAA long has been an outspoken organization on the impact of the shortage of IT workers—whether in computer security or any of the other IT occupations. Our groundbreaking studies on the IT workforce shortage—"Help Wanted"—have defined the debate and brought national attention to the need for new solutions to meet the current and projected shortages of IT workers. We believe it is important to assess the need for and train information security specialists, and believe it is equally important to train every worker about how to protect systems. We know from the recent denial of service attacks last month that systems are only as strong as the weakest link-whether it's people or technology.

We have planned a security skills set study to determine what the critical skills are, and will then set out to compare those needs with courses taught at the university level in an effort to determine which programs are strong producers. We encourage the development of "university excellence centers" in this arena, and also advocate funding for scholarships to study information security.

The challenge to find InfoSec workers is enormous, because they frequently require additional training and education beyond what is normally achieved by IT workers. Many of the positions involving InfoSec require US citizenship, particularly

those within the federal government, so using immigrants or outsourcing the projects to other countries is not an option.

Best Practices: We are committed to promoting best practices for information security, and look to partners in many vertical sectors in order to leverage existing work in this area. In addition, our industry is committed to working with the government—whether at the federal, state or local levels. For example, we are working with the Federal Government's CIO Council on efforts to share industry's best information security practices with CIOs across departments and agencies. At the same time, industry is listening to best practices developed by the government. This exchange of information will help industry and government alike in creating solutions without reinventing the wheel.

While we strongly endorse best practices, we strongly discourage the setting of "standards." Why?

Broadly, the IT industry often sees standards as a snapshot of technology at a given moment, creating the risks that technology becomes frozen in place, or that participants coalesce around the "wrong" standards. It is also critical that best practices are developed the way much of the Internet and surrounding technologies have progressed—through "de facto" standards being established without burdensome technical rules or regulations. While ITAA acknowledges the desire within the Federal government to achieve interoperability of products and systems through standard-setting efforts, we believe that the IT industry can address this simply by responding to the marketplace demand. The market place has allowed the best technologies to rise to the top, and there is no reason to treat information security practices differently.

Research and Development: While the information technology industry clearly is spending hundreds of millions if not billions on research and development efforts-maintaining our nation's role as the leader in information technology products and services-there are gaps in R&D. Industry clearly focuses on R&D projects that are likely to lead to real products. Government, mainly in the Department of Defense, focuses its information security R&D spending on defense and national security issues. We believe that in between industry's market-driven R&D and government's defense-oriented R&D projects, gaps may be emerging that no market forces or government mandates will address.

ITAA and our member companies actively support the President's call for an Institute for Information Infrastructure Protection. This institute, under consideration by the President's Committee of Advisors on Science and Technology, will focus limited government funding on targeted R&D projects conducted through consortia of industry, academia and government. We continue to support the creation of the Institute and hope the Congress will approve the $50 million fiscal year 2001 request for its establishment.

International: In our work with members of the information technology industry and other industries, including financial services, banking, energy, transportation, and others, one clear message constantly emerges: information security must be addressed as an international issue. American companies increasingly are global corporations, with partners, suppliers and customers located around the world. This global business environment has only been accented by the emergence of on-line commerce—business-to-business and business-to-consumer alike.

Addressing information security on a global level clearly raises questions. Many within the defense, national security and intelligence communities rightly raise concerns about what international actually means. Yet, we must address these questions with solutions and not simply ignore the international arena. Again, we are only as strong as our weakest link. To enable the dialogue that is needed in this area, ITAA will be announcing soon the first Global Information Security Summit to be held this fall. This event will bring together industry, government and academia representatives from around the world to begin the process of addressing these international questions.

Information Sharing: Last month, I and numerous executives from my industry met with President Clinton to discuss solutions to combating security threats. We committed to the President that we would create a mechanism for sharing information.

There are still unanswered questions as to what the mechanism will look like—how formal will it be? With whom will we share information? How will such a mechanism be funded and operated? These are important questions, which need answers.

One other issue is important to raise concerning information sharing. During the Y2K rollover, the Federal government's Information Coordination Center (ICC) played a critical role in ensuring a smooth process. At the ICC, government and industry stood side-by-side in an unprecedented effort to ensure the continuity of oper-

ations of America's critical infrastructures and the sustained health of our national economy.

As we begin to share information within our industry and develop the process for sharing across industries and with government, we see a potential role for the ICC in enabling this collaboration. Yet, the Federal government's approximate $40 million investment in the ICC is at high-risk of being discarded. As we speak, the OMB is moving quickly to dismantle the ICC, divvy up the ''goods,'' and leave nothing behind. We have asked OMB Director Lew to reconsider this plan to dismantle. The plan moves forward. We now ask you to help us ask OMB to ensure it has clearly identified all possibilities for the ICC-particularly in an information security capacity—before the ICC is gone.

Which brings us to the question today's hearing asks.

BARRIERS TO INFOSEC IMPLEMENTATION

Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. Information sharing is a risky proposition with less than clear benefits. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments. Nor would they risk voluntarily opening themselves up to bogus but costly and time-consuming litigation. Releasing information about security breaches or vulnerabilities in their systems presents just such risks. Negative publicity or exposure as a result of reports of information infrastructure violations could lead to threats to investor—or worse—consumer confidence in a company's products. Companies also fear revealing trade secrets to competitors, and are understandably reluctant to share such proprietary information. They also fear sharing this information, particularly with government, may lead to increased regulation of the industry or of Electronic Commerce in general.

These concerns are relevant whether we are talking about inter-industry, cross-industry, or industry/government information sharing. Combine this with a historic lack of trust towards law enforcement, or a concern that company systems may become caught up in an investigation and thus lose production/development time, and many companies find it easier to keep quiet and absorb the pain inflicted by intrusions, even at substantial cost. I also would be remiss if I did not remind the committee of a company's need to protect individual customers' privacy. Industry fears that privacy breaches on innocent customers might inadvertently occur during investigations.

Few high tech companies are interested in being perceived by their customers as the active agents of law enforcement. Agencies, meanwhile, are often viewed as demanding this type of information from the private sector but giving little back in return. Let me be blunt. Information sharing cannot be a one-way street.

TARGETED SOLUTIONS ARE POSSIBLE

In many ways, solutions to information security challenges are no different than any other Internet-related policy issue. Regulation is not the answer. Industry leadership has been the hallmark of the ubiquitous success of our sector, and we firmly support the current beliefs held by most in Congress and outlined in the Administration's 1997 plan, ''A Framework for Electronic Commerce,'' which advocates market-driven, industry led, free market approach to the Internet and E-Commerce. These same principles must be applied in the realm of information security.

Over the past two years, ITAA, its members and the IT industry have begun to develop collegial and constructive relationships with the leadership and staff of the Department of Justice (DOJ), the National Security Council (NSC), the National Security Agency (NSA), the National Information Protection Center (NIPC), the Critical Information Assurance Office (CIAO), the Commerce Department (DOC), NTIA and the Critical Information Infrastructure Assurance Program Office (CIIAP) at NTIA in their capacity as the lead agency for our industry. While significant, positive levels of trust, cooperation and communication have been developing; the important work that must be done has barely started. This is not because of any lack of desire or ability on behalf of NTIA or the CIIAP Office, but because they have been asked to do their job without the necessary resources. They lack even the minimum funding and support that is necessary for them to carry out their mission. ITAA and our members will continue to look forward to cooperating with all agencies and elements of government to meet the Infosec challenges. Yet we feel that NTIA is the proper representative to work with our industry to begin to build the necessary levels of cooperation to help develop the National Infrastructure Protection Plan. Within DOC, NTIA has the knowledge of and experience and relation-

ships with the IT and Communications industries that are necessary. It is essential that the necessary programmatic funding for lead agency activities be appropriated to the NTIA to carry out its mission. $3.5 million (amount of current request for NTIA lead agency activities) is a small price to pay for getting these important programs moving down the track.

Part of the answer will require new approaches to the Freedom of Information Act (FOIA), one of the biggest roadblocks. Companies worry that if information sharing with government really becomes a two-way street, FOIA requests for information they have provided to an agency could prove embarrassing and probably costly. Many in industry believe that freedom from FOIA concerns is the most formidable obstacle, and that an exemption for this type of information sharing is the only option.

ITAA's collaborative partnership with the Department of Justice, the "Cybercitizen Partnership" is developing an educational program to teach children that ethical, moral responsibility exists in the virtual world as it does in the real world. The efforts of the Partnership will reduce the potential of children to engage in cybercrime. A modest amount of funding for this type of awareness campaign would go a long way towards teaching the first generation of true cybercitizens, and our future workforce, about the realities and consequences of misbehavior online.

Funding will also help in the areas of workforce development and research. We have a critical shortage of information technology professionals generally and information security specialists specifically. The $25 million set aside in the fiscal year 2001 budget for the Federal Cyber Services Training and Education Initiative should prove most helpful. The fellowship program outlined in HR 2413, the Computer Security Enhancement Act of 1999, to increase the number of IT skilled workers in the workforce, is something we also support.

The President's proposed Institute for Information Infrastructure Protection, a federal research and development facility, should likewise prove beneficial to the extent that it is responsive to the marketplace. The best way to assure the Institute's relevance is to build it on a broad collaboration between government and industry, focusing on technology certainly but not losing sight of the critical importance of people and processes to the information security equation.

CONCLUSION

In all honesty, we at ITAA face a daunting job of convincing the IT industry to work with federal agencies on these initiatives, even under the best of circumstances. The most important aspect of successful information sharing lies in the breadth and depth of the sharing. We must do more than industry only communications. There must be inter-industry, cross-industry and industry/government cooperation on InfoSec. Nothing less will get the job done. It is a challenge we must step up to if we are to achieve any degree of success in opening lines of communication. Our industry continues to have reservations about working too closely with the federal law enforcement and national security community, and has concerns about jeopardizing business concerns by sharing information on security issues.

Without overstepping its boundaries, there are ways the government can create a friendlier atmosphere for information sharing as well as increase our successes in this arena.

Thank you and I would welcome any questions from the Committee.

Senator KYL. Well, both of you have certainly summarized the issues well. Let me begin, Mr. Miller, by asking a couple of very specific questions.

As you know, the FBI is the primary law enforcement entity charged with the investigation and prosecution of crimes in this case. Is the NIPC's placement in the FBI, from your perspective, a show-stopper for the partnership that you testified we need to create between government and industry?

Mr. MILLER. I would recommend it not be within the FBI. Show-stopper may be too strong a term, Senator, but I think that as much respect as the business community has for the FBI, they are clearly more comfortable working with other agencies. For example, we work very closely with the Department of Commerce. That is the sector coordinator position we were given that came out of the Department of Commerce.

So perhaps in terms of information sharing, while we receive that law enforcement and national security officials will always be a central part of it, as long as this remains within the FBI, then it will be seen exclusively by most people, rightly or wrongly, as a law enforcement agency, not as an information sharing organization.

And as Senator Grassley pointed out in his comments, particularly when you don't have major agencies such as the Department of the Treasury and the Department of Commerce even currently playing a role within the NIPC, then again the perception from the outside, Senator, is this is purely a law enforcement organization, not a general information sharing organization. My guess is that industry would be more comfortable if it were not located within the FBI.

Senator KYL. Of course, to the extent that is a law enforcement function, the FBI has got to be involved, and you are not suggesting otherwise.

Mr. MILLER. Absolutely not.

Senator KYL. I think part of the problem is the Administration has frankly not been encouraging enough of Treasury and Commerce to participate in this. Perhaps more encouragement there could bring a larger role for Commerce and Treasury and some of the other agencies of the Government.

Mr. MILLER. Well, one of the things I have suggested, Senator, in testimony on the other side of Capitol Hill is the need for an InfoSec czar similar to the role that John Koskinen played, a small, lean, mean organization reporting directly into the President and Vice President and the National Economic Council who would be able to more clearly rationalize the Government agencies.

Frankly, from the outside, it looks very, very confusing. In fact, we could probably fill up the whole wall behind you with charts about everybody inside the Government who is dealing with information security not just internally, but also to the external audience, the business community, the average citizen, consumers, State and local governments.

And perhaps a Koskinen-like individual—John Koskinen served that role, of course, for Y2K, who would be seen and trusted both inside the Government and also outside, again not to set up his or her own bureaucracy but as a primary point of contact externally with the various parts of the private sector, State and local government and internationally, and then internally could help to at least—to the outside world—paint a clearer face as to what the position would be, might be very helpful.

Senator KYL. OK; I take your suggestion. Two other very specific questions. Do you see a need for modifications to antitrust legislation to encourage sharing among competitors?

Mr. MILLER. Our legal committee at ITAA is examining that. We do believe that probably it will be necessary. As you know, Senator, during the Y2K debate over the past several years, Congress did pass the Information Readiness and Disclosure Act which did relieve any lingering concerns that legal departments and general counsels and outside counsels had about firms sharing information, under your leadership and many members of this committee. That was an important bill that helped to promote information sharing.

Even though companies were told by the Department of Justice they could industry by industry go in for an exemption, and some industries did, that turned out to be a long, laborious process. So legislation was very key. So we are now in our legal committee examining the possibility and have had some dialog with the Administration and would be glad to carry on a dialog with you and your staff on that also.

Senator KYL. We are eager to get your recommendation on that.

Then a final question, and this will be a bridge to Mr. Pethia. With respect to the Freedom of Information Act, is it fair to say that we won't have adequate information sharing until we offer an exemption to FOIA for critical information infrastructure protection?

Mr. MILLER. Absolutely. As long as companies believe that by cooperating with government they are facing the risk of very sensitive and confidential information about proprietary secrets or about customer records, while however well-intentioned end up in the public record, that is going to be, to use your phrase, a showstopper.

Senator KYL. Now, Mr. Pethia, we have heard about market forces that help private companies secure networks, but a lot of the attacks have been through universities due to their traditional high-capacity, low-security networks. What do you suggest we do to encourage or hold accountable universities to take security more seriously?

Mr. PETHIA. An interesting question. I think overall universities are certainly a piece of this, but I think they are just the beginning of what we are going to see over the next few years, which is going to be hundreds of thousands of organizations that are vulnerable to this kind of attack.

I think overall we have to begin to help people understand, first of all, the liability that these organizations have if they leave their systems open and repeatedly can be used as platforms to launch new forms of attack. And I think more than anything else, that will eventually bring the kinds of controls that we need to have. I don't know how to do it any other way. Until individual organizations begin to see that there is some price to pay for lax security, I think we are going to have that problem.

The bigger problem I see, however, is on the other side, and that is on the technology producer side. I think the fact is today many of the systems we have out there today are simply too complex for today's user environment to effectively deal with.

One of the things I would like to say is that the Internet was originally built by the technical wizards for the technical wizards, and we still have a lot of the old software, the same mechanisms in place today that we had 10 years ago. Today, computers, even sophisticated devices like firewalls and routers, are becoming consumer items.

We don't expect everyone who drives an automobile to be a master mechanic, and we shouldn't expect everyone who uses a computer that could be used as an attack platform to be a master systems engineer. So what we need to fix this problem long term is better technology, technology that is matched to the capability of today's users.

Senator KYL. And I think the question that, Mr. Miller, your folks are going to have to grapple with is the issue of whether or not, going back to the weakest link notation, a university, a company, an individual who knowingly or willingly avoids known fixes in a system allows that system to be used for malicious purposes that significantly injures others—whether there is a potential liability there, and therefore whether there is going to be some obligation to take some reasonable steps.

Do either of you have a comment on where that whole thing is headed?

Mr. MILLER. I think it is a combination of both. No. 1, it is education. At the meeting that Mr. Pethia and I attended with the President at the White House, for example, following the initial denial of service attacks, one of the major companies reported that every time they did a major installation they went in 60 days later to see how the installation was working and they found that in over 35 percent of the cases the customer never turned on the security they had been given, which the President then analogized to people who buy briefcases that have 000 locks on them and never change the lock from 000.

So in that case, education is important. Maybe the customer thought it was too difficult, which Mr. Pethia is suggesting might be the case, or maybe they just didn't give it any priority and therefore they didn't do it. So education which is important is there.

But, No. 2, there are going to be negative incentives, too, I think, as you are suggesting, Senator. I think there are going to be down the road, maybe sooner than we think—lawsuits, various liability issues raised, shareholder lawsuits, et cetera, that may arise. Now, it is interesting that one of the organizations, I think, very positive, by the way, that has gotten involved is the Institute of Internal Auditors. They have become very involved in this issue.

In fact, they are going to be holding a series of briefings and meetings around the country that is being organized in conjunction with the CIAO office, in which we are also participating. Clearly, an auditor has a lot of impact on a company. If an auditor says, I am not going to sign off on your audit or I am not going to approve your audit until I am convinced that you have instituted the appropriate security mechanisms, that is important.

Similarly, the insurance industry. Many insurance companies were writing service interruption insurance for Web-based companies without ever asking the tough question: by the way, have you done anything to be secure? And then there is some business interruption because someone takes down their website. The insured comes forward to file a claim and the risk managers says, "Oh, we forgot to ask you, didn't we, whether you really had any protection?" So the insurance companies are now starting to change their tune and putting pressure on companies.

So I think, similar to Y2K, you are seeing a lot of outside pressures in the marketplace—insurance, lawyers, auditors, customers. Obviously, if customers go back to certain well-known online websites and they are down all the time, eventually the customers will move away, the investors will move away. So all those market forces are starting to work, but it is going to be a slow process be-

cause I would say that maybe for most companies up until the recent denial of service attacks, information security was number 11 on the 10 critical things they had to do.

I think maybe now it is number 6 or number 5. It has moved up the food chain, but it isn't up to number 2 or number 3 yet where it needs to be. And what that is going to take, Senator, just as Y2K did, is CEO and COO and CFO commitment, board of directors commitment. It is not the MIS director, it is not the technical person, it is not the chief technology officer. Those people are important in terms of figuring out the correct technological solution, as Mr. Pethia was suggesting.

But in terms of putting the dollars on the table in terms of the commitment of resources in terms of the priority, that has to come from the top, whether you are talking about a university president, whether you are talking about a corporation, whether you are talking about a nonprofit, whether you are talking about State and local government. The commitment has to come from the top for information security to rise to the level where it needs to be.

Mr. PETHIA. I would like to build on Harris' statement for just a minute.

Senator KYL. Sure.

Mr. PETHIA. The real scary thing about the distributed denial of service attacks in February is not that they caused damage, but for the first time in the history of the Internet it became crystal clear that there is nothing that an organization can do to protect itself from this kind of attack.

So for the first time we have taken the traditional risk management model and stood it on its head. No matter what I do within my organization, no matter how much I invest in security, no matter how strong the doors are to my organization, I am still vulnerable to an attack from some 15-year-old who picks up a piece of technology off the network. That can't be the right technical answer. We simply cannot manage risk in any effective way.

So what we need to push toward is better underlying technology in the Internet. There are groups like the Internet Engineering Task Force that are developing improved security standards, but yet industry is very slow to adopt them. Internet Protocol Version 6 which has been available now for well over a year has a lot of real strong security controls that could help us deal with a lot of this problem, but its deployment is probably still 2 or 3 years away because industry is simply not picking up the banner and running forward.

There is the place where I think the community has already come together. They have vetted the solution. It is a solution that is acceptable to all of them. That is how the Internet Engineering Task Force works, and here is the place where I think government perhaps could exert some influence to try to accelerate the deployment of what industry has already agreed is an effective new standard.

Senator KYL. How could government do that?

Mr. PETHIA. Well, I don't know the exact mechanism to do that, but there again certainly within the Federal Government, as the Federal Government is a purchaser of large amounts of information

technology, it could begin to demand that as it buys new products those new products incorporate these new features.

Senator KYL. Well, that is certainly true. The confusing thing to me is from my own perspective I would rather see the private sector evolve legally as well as technologically to put its own numerous kinds of pressure on businesses to do business in a proper way that recognizes industry standards to which people are held accountable for not availing themselves of equipment to meet those standards. The Government's primary role is when there is a national security type of issue involved, and that is where the Government could actually mandate something.

The problem is that you have here a highway used by everybody. The worldwide Internet is basically open to anybody and you could have anything from a terrorist attack to a very specific attack on some national security component of the country, either government or nongovernment, as well as financial crimes and just plain hacking, all using the same medium, in effect.

So it is kind of hard to clearly define when the Government's mandating role is appropriate and when instead it should just rely on the private sector itself to evolve the legal mechanisms to provide the enforcement.

Mr. Miller.

Mr. MILLER. I would agree with you, Senator. I am very, very reluctant to see government try to set standards, but let me give you a couple of examples of where collaboration may work out well.

Our association is working currently with the Federal Chief Information Officer Council of the Federal Government, which is the CIO's of the 24 largest Federal agencies established under the Clinger-Cohen legislation several years back. They have decided within their leadership role within the Government IT sector to try to develop best practices so that they, as customers, can be smarter about how to do that.

They have come to us to be an information sharing resource, not that we are going to dictate to the Government what their best practices are, but they want to learn and educate themselves by establishing a very open and frank dialog between industry and government, which by the way is going to have to be ongoing because today's countermeasure is frequently overcome by some new threat and it becomes an escalating arms race.

So we are having a couple of meetings upcoming with the Federal CIO Council and other CIO's. It is quite possible that those best practices will get more widely adopted than just within the Federal Government, for instance. Similarly, in the meeting we had with President Clinton on February 15, we in industry committed to setting up a more effective information sharing mechanism within the IT industry and across industries, trying to expand on the excellent work that Mr. Pethia's organization does. But we also committed to the President to work on best practices.

So I think that you are going to see this accelerating toward best practices. Is it going to be standards that someone can go pull down off the shelf and say, "OK, I know exactly how big, how tall, how small?" No, but I think you are seeing a lot more pressure toward realizing that because we are all in this together, as you sug-

gested, we are living in the same Internet world, we have to have some best practices.

One final point, Mr. Chairman, in this area is a lot of these challenges are not technological, they are personnel. If I install a security system at your house and you don't punch in those four digits before you go to sleep at night, I might as well have not installed it. Similarly, the example I gave before: if companies have security installed and they never turn it on, they might as well not have it.

As Director Freeh reported, a huge percentage of the information security problems come internally, not from external threats, not from terrorists or criminals, but internally. So personnel and human resource factors here are exceptionally important, and those are the kinds of things that industry also needs to work on collaboratively together.

We, for example, are working with Marymount University here in northern Virginia on a program in early September which is going to try to figure out how to better educate college students on basic procedures. Whether you are going to be a computer specialist or just someone who uses the computer for word processing and spread sheets, you have to practice good cyber hygiene the same way that the MIS director does or the same way that someone who has a much more sensitive role in government does. Otherwise, the whole system can be threatened.

Senator KYL. One idea, too, with regard to the universities is because of the Federal funding link to the universities, there could be requirements placed to adhere to at least certain protocols or standards in connection with the use of those university computer systems.

There is much more we could get into. I would invite both of you to continue to communicate with our subcommittee because we are going to be developing legislation. We will need your continued input and advice. We will maintain that communication because you both emphasized the need for that. I totally agree with it.

The only thing I would say in closing, and it goes back to a point I made with the Director, is my first 20 years were in the private sector and I am very private sector-oriented, but there are some trust barriers that need to be breached here on both sides. And I would just suggest that you think about how to communicate to some of the folks in the private sector how sometimes actually being involved in a law enforcement aspect of something provides better protection than before that process actually begins. So it is not something necessarily to be feared.

But, of course, we all appreciate the other concerns about snooping and all of that kind of thing. In any event, it is just one more way to try to break down the barriers for that two-way communication that we have all been searching for.

Mr. MILLER. Well, we would be glad, Senator, to work with you and your colleagues to even have a dialog not just with Attorney General Reno and others but with your committee, if you thought that would be appropriate, where you could help to deliver that message.

One of the ways that I got a commitment from my board of directors to focus on this issue so much was 2 years ago I asked a senior

official from the FBI to come out and do a confidential briefing for my board of directors. And it got their attention when they heard close up and personal what was going on in the industry. So perhaps not just our dialoging with the Attorney General and the Department of Commerce, but maybe with leaders in Congress would be helpful. And I would be glad to facilitate such a meeting if you and your subcommittee would be interested.

Senator KYL. I, for one, would be delighted to do that, and I would just encourage both of you. Any suggestions, proactive, please get them to us because in many ways this is a very exciting challenge and there are some wonderful opportunities here. But we have got to attend to them soon or we are going to continue to face significant risk.

Mr. PETHIA. We work closely with the FBI and the NIPC. In fact, we have representatives from the FBI actually physically located in our facility, and we always encourage people who report incidents to us to report to law enforcement as well. I think lack of trust is part of it, but there is also a tremendous lack of understanding.

We recently met with Michael Vatis, the director of the NIPC. They will be working with us to really help people, inform people, produce documents and seminars that we can do together to inform people of what they can expect to have happen when they do report to the FBI.

One of the things that I think is important to remember is that the Internet today in this country alone is growing by hundreds of thousands of users everyday, and that is a huge population of people to pull up a learning curve and to make them feel comfortable with this new world that they are in and dealing with law enforcement organizations that they probably have near dealt with before. I think that is the big challenge, pulling all those people up that learning curve.

Senator KYL. Well, you have both made excellent points. I appreciate your testimony here. We will look forward to continuing dialog with you.

I would note that the subcommittee record will be kept open for a week if any of you would like to submit anything else or if any members of the panel would like to submit any additional questions for the record.

With that, I thank you and adjourn this hearing.

[Whereupon, at 11:52 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS AND ANSWERS

RESPONSES OF LOUIS J. FREEH TO QUESTION FROM SENATOR JON KYL

Question 1. Is the NIPC able to provide indications and warnings of an attack? For example, does the Center have the ability to detect anomalous activity or patterns in key communications nodes that might indicate something is about to happen?

Answer 1. The NIPC's ability to perform "indications and warning" is dependent first and foremost on its ability to quickly gather information from multiple sources about an ongoing or imminent attack (whether an intrusion, a virus, a denial of service, or other form of attack). The NIPC does not operate any detection mechanisms on any government or civilian systems. Thus, we do not get "indications" in an automated sense from any detection devices. In this sense, I&W in the cyber world is very different from I&W in the nuclear missile or conventional weapons world, where radars and other devices can provide advanced warning of an attack. Rather, we get relevant information from intelligence sources, criminal investigations, "open sources" (such as media and the Internet), and from industry and government contacts. We "detect" anomalous activity in key communications nodes only if the owner/operator of that node detects it and informs the NIPC, an FBI Field Office, or another agency, or if we learn through criminal investigation or intelligence sources that the node is being attacked. The key to the NIPC's ability to do this is the development of connectivity and close interaction with numerous Defense and Intelligence Watch centers, FBI Field Offices, other Law Enforcement organizations, computer anti-virus association groups, private and public Computer Incident Response Teams (CIRTs) and Computer Emergency Response Teams (CERTs), foreign law enforcement agencies, and private industry (both individual companies and information sharing organizations). Over the past two years, the NIPC has made substantial progress in developing these relationships, but this is a continuing task and more work remains to be done. One of the main reasons for our extensive outreach programs is to build trust and willingness on the part of private companies to report cyber incidents to us, and these efforts are bearing fruit. In addition, PDD–63 directs other federal agencies to report incidents to the NIPC directly. Many agencies are doing this, but there is room for improvement with others. In addition to reports from companies and agencies, the NIPC Watch actively scans all available governmental and private sector sources for reports or information regarding cyber activity, and interacts throughout each day with other watch centers to share information.

Once information (or "indications") of an attack is received and analyzed, the NIPC can issue a warning, alert, or advisory through numerous means, depending on the appropriate audience. Warnings can be issued to specific targeted companies through FBI Field Offices or by the watch directly; other federal agencies can be notified by e-mail, secure facsimile, and telex; state and local law enforcement can be warned by NLETS; industry can be warned through InfraGard secure email and website and through ANSIR (an e-mail system that reaches tens of thousands of companies); and the general pubic can be warned via the NIPC webpage and the news media. All of these mechanisms have been used numerous times (as discussed in the answer to the next question).

Senator Kyl's question goes to the heart of I&W in the cyber world: should the Nation have the capability to detect intrusions into government or private sector systems in an automated fashion, without having to rely on human detection and reporting? The controversy attending the Administration's recent "FIDNET" initia-

tive, which is a limited proposal to place automated intrusion detection devices on federal agency networks, identified many of the privacy and other issues such a system would raise, particularly if it were extended to privately owned networks. The government's approach at the present time is to encourage industry to protect and monitor its own systems, and to report anomalous activity voluntarily. The NIPC works within that overall policy to encourage private sector reporting as a critical part of its I&W. Examples of this include InfraGard and the incident reporting pilot program we have developed with the energy sector through the North American Electrical Reliability Council (NERC).

Question 2. How many warnings has the NIPC issued which were developed through the Centers's own analysis of activity?

Answer 2. Of the 54 tactical warning products disseminated since the NIPC was established in February 1998, all were developed in whole or in part through the Center's organic analytical capability and analysis of activity. Some of these products were initiated by the NIPC (e.g., the BAT/Firkin Worm, also known as the "911" Worm), while others built upon basic analysis initiated elsewhere (e.g., the NIPC assessments of Distributed Denial of Service tools). We cannot put a precise figure on the relative contributions, since these are all community-collaborative products. In performing analyses and issuing warnings, the NIPC works closely with other government agencies, private sector organizations such as CERT (which is an FBI contractor), and the SANS institute, and academic institutions.

In addition to warning products, the Center has produced hundreds of non-warning informational products. Since 1998 the NIPC has produced 301 daily reports, 30 CyberNotes (a summary and analysis of technical exploits and vulnerabilities), 51 Critical Infrastructure Developments reports (a report on recent cyber-related issues and incidents), and five IP Digests (a periodic, in-depth analysis of cyber threats and vulnerabilities). Versions of these analytical products go to private industry, to the Intelligence Community, other federal agencies (including law enforcement), and to criminal investigators.

Question 3. What-other agencies do you see playing a significant role in the area of computer crime investigations?

Answer 3. Cyber crime is an issue that concerns not just the FBI, and, not just law enforcement generally. Indeed, "cyber crime" in itself should be seen as part of a broader array of cyber threats, including cyber terrorism, cyber espionage, and information warfare, since all are closely related and often difficult to distinguish at the outset of an incident. As a result, cyber threats are of great concern to numerous federal agencies, including the Defense, Intelligence, and Law Enforcement Communities and to civilian "Lead Agencies" under PDD–63; to state and local governments, including law enforcement; and, of course, to the private sector. It is because of this wide-ranging interest that the NIPC was established as an interagency center. The NIPC provides a locus and mechanism for coordinating the expertise and roles of many agencies, and facilitates information sharing and operational coordination. The NIPC works closely on investigative matters with many law enforcement agencies, including: the Secret Service, Internal Revenue Service (IRS), Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), United States Air Force Office of Special Investigations (AFOSI), Defense Criminal Investigative Service (DCIS), National Aeronautics and Space Administration Office of Inspector General (NASA OIG), Department of Energy (DOE), state and local law enforcement, the Intelligence Community, as well as foreign law enforcement agencies through FBI Legal Attaches (LEGATS).

Question 4. Are there reasons, other than funding, which have caused other agencies to pull their personnel out of the NIPC? For example does FBI management at the Center recognize the expertise of the other agencies and allow them to fully participate?

Answer 4. One of the difficulties in attempting to operate an interagency Center is ensuring that all relevant agencies participate. Agencies have not received direct funding to participate in the Center, and so must take detailees to the NIPC out of existing personnel resources. In addition, personnel with cyber expertise are unfortunately in very short supply, meaning that agencies must commit to take scarce resources and send them outside their agencies. Despite these impediments, numerous agencies have sent detailees to the NIPC, including: Defense/Office of the Secretary of Defense; Central Intelligence Agency; National Security Agency; Air Force Office of Special Investigations; U.S. Navy; U.S. Army; U.S. Postal Service; Defense Criminal Investigative Service; General Services Administration; U.S. Air Intelligence Agency; Department of Commerce, and the Tuscaloosa, AL Sheriff's office. In addition, we have foreign liaison representatives from two allied countries who assist in coordinating international activities with our counterparts. A representa-

tive from FAA is also scheduled to start at the end of June. Additional representative from DoD, CIA, and NSA are also slated to arrive in the near future. We are also expecting representatives from local Washington area police departments on a part-time basis.

Some agencies were represented earlier but do not currently have representatives. Circumstances necessitated the recall of the first State Department representative. State agreed to do so, and has committed to NIPC that it would replace him with two new representatives. DoE's first representative rotated back after more than two years. NIPC's understanding as to why this representative rotated back is that he was at NIPC for a lengthy time and was needed at DoE headquarters to assist in a DoE reorganization. DoE has committed to replacing that detailee.

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has not yet committed to replacing them. Secret Service has not provided any written explanation for this, but in oral discussions, Secret Service officials stated that USSS was not getting additional funding for its electronic crimes program despite its participation in NIPC; the FBI was receiving more media attention in the cyber crime area; and NIPC had not "referred" cases to Secret Service for investigation. NIPC offered any support it could give to Secret Service in addressing budget requests; noted that NIPC public statements often referred to partnership with USSS; and offered to do more to support USSS initiatives with public statements and case analyses. NIPC also stated (as discussed further below) that its role is not to create and "refer' 'cases; rather, cases generally originate in Field Offices, and FBI and Secret Service field offices frequently work computer crime cases together.

NIPC fully recognizes the value other agencies bring to the cyber crime and infrastructure protection mission. That is why NIPC is an interagency Center, and has senior managers from other agencies in addition to investigators and analysts. For instance, the NIPC Deputy Director is from DoD/OSD; the Section Chief of the Analysis and Warning Section is from CIA; the Assistant Section Chief of the Computer Investigations and Operations Section is from Air Force OSI; the Unit Chief of the Analysis and Information Sharing Unit is from NSA; and the Unit Chief of the Watch and Warning Unit is from the U.S. Navy. Secret Service formally occupied the position of Assistant Section Chief of the Training, Outreach, and Strategy Section. Recognition of the need for other agency participation is also what drives NIPC to continually seek additional representatives from other agencies. It is also reflected in the numerous joint investigations that NIPC and FBI Field Offices have been involved in with other agencies (as discussed further below).

Question 5. How many criminal investigations have been referred from the NIPC to these other agencies? Does the Center have operating procedures to refer a case to another agency?

Answer 5. As a general matter, the NIPC does not "refer" cases. Cases are normally initiated by a field office, whether a Field Office of the FBI, the Secret Service, another federal agency, or a state or local law enforcement agency. NIPC is the "program manager" of the FBI's computer intrusion investigative program, and so receives information about cases directly from the FBI Field Offices. Under PDD 63, other agencies are also supposed to report information about cyber incidents to the NIPC. Sometimes, NIPC will receive the first report of a cyber incident from a private company, a government agency, or another source, and contact the appropriate FBI Field Office. If another agency has concurrent investigative jurisdiction or some other non-investigative interest, that agency will also be contacted (either by the FBI Field Office of the NIPC. Where joint jurisdiction exists, the FBI field office may work jointly with the relevant other agencies (as discussed further below).

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

There have been, however, several instances in which the NIPC or an FBI field office has contacted another agency to determine if that agency wanted to conduct an investigation either jointly or separately, but that agency declined. A couple of examples are listed below.

In May 2000, the FBIs Detroit Field Office referred a complaint to the local Secret Service office regarding a denial of service attack against NHL.com, going so far as to transfer the call from the FBI field office to the Secret Service field office. The Secret Service told the complainant that no one was in the office to receive the complaint due to a visit of Texas Governor George W. Bush to Michigan. The complain-

ant then called the FBI again and the Detroit Field Office took the complaint and assigned the matter for investigation.

Also in May 2000, based on FBI source information, the NIPC notified the USSS headquarters that there may be a vulnerability with the White House Webpage that gave the public access to all the files on that server. The USSS advised that the system administrator may already be aware of this. Neither the NIPC nor the FBI's Washington Field Office has heard back from the USSS regarding this matter.

In another instance, the FBI's Williamsport, Resident Agency, part of the Philadelphia Field Office, opened an investigation into a series of computer intrusion into 10 companies resulting in the loss of approximately 28,000 credit card numbers. During the initial investigation, the FBI discovered that one of the victims located in Buffalo, NY, had contacted the Secret Service and the USSS had opened a case pertaining to the intrusion against the single victim company, but was not investigating the larger set of thefts. The FBI contacted the Secret Service Division in Buffalo, NY to coordinate the case, since USSS already had a pending investigation. The FBI was told that due to the Security Detail Duties for the First Lady, the USSS would be unable to coordinate at the present time with the FBI on the case.

Question 6. In previous testimony before this subcommittee Mr. Vatis has stated that the NIPC has referred approximately 800 cases for criminal investigation. How many of these 800 cases actually involved a real threat to our nation's critical infrastructure? Would you categorize the recent Denial of Service attacks launched last month as an attack on our nation's critical infrastructure?

Answer 6. In previous testimony before the subcommittee, the approximate 800 number of cases that Mr. Vatis referenced were not cases the NIPC "referred," but was the number of computer intrusion, denial of service, or virus cases pending in FBI field offices at the time of testimony. As of May 1, 2000 there were 1,072 pending investigative cases.

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus of these 1,072 cases, there is no methodology to determine which ultimately constitute a threat to our nation's critical infrastructure. However, we can cite several examples.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

Question 7. Besides Solar Sunrise and Moonlight Maze, what other joint investigations can you point to that demonstrate successful interagency cooperation?

Answer 7. Since the founding of the NIPC in February 1998, there are numerous cases which have demonstrated successful interagency cooperation other than the significant Solar Sunrise and Moonlight Maze cases. The importance of these two cases should not be overlooked, however. Both represent significant milestones in

building awareness of the cyber threat among federal agencies and policymakers, demonstrated significant vulnerabilities in DoD and other government systems, and provided opportunities to test and improve the NIPC's processes for interagency coordination.

The following cases represent a small sample of these cases which have been successfully worked with other agencies:

DDOS: Numerous Internet commerce sites have been victimized by DDOS attacks since February 7, 2000. These DDOS attacks prevented the victims from offering their web services on the Internet to legitimate users. A DDOS attack uses compromised computer networks to "flood" a victim's computer network with massive amounts of data, which causes the victim's computer network to become overwhelmed and to stop operating. The DDOS attack investigation are investigations in seven FBI field offices, five overseas Legal Attache offices, other government agencies such as NASA, as well as the Royal Canadian Mounted Police. Reflecting the extraordinary level of cooperation on these investigations, on April 15, 2000, the Canadian officials arrested a juvenile charging him with one of the attacks.

Curador: On March 1, 2000, a computer hacker using the name, "Curador", allegedly compromised multiple E-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers. Thousands of credit card numbers and expiration dates were posted to various Internet websites. On March 9, 2000, InternetNews reported that Curador stated, "Law enforcement couldn't hack their way out of a wet paper bag. They're people who get paid to do nothing. They never actually catch anybody." After an extensive international investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (UK) Police Service in a search at the residence of Curador; Curador, age 18, was arrested in the UK, along with an apparent co-conspirator under the Computer Misuse Act 1990. Under United Kingdom law, both males have been dealt with as adults. Loss estimates are still being determined.

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Burns: In August 1998, the FBI initiated an investigation on an individual only known as "zyklon," who conducted numerous computer intrusions to various computer systems causing damages to websites, and system files. The case was worked in cooperation with the Virginia State Police. The investigation identified zyklon to be Eric Burns of Shoreline, Washington. In February 1999, following an execution of a search warrant, Burns confessed to the intrusions. In May 1999, Burns also gained unauthorized access and defaced the webpage for the White House website. At that point the FBI began working with the U.S. Secret Service on the case. In September 1999, Burns pleaded guilty to one count for violation of Title 18 USC Section 1030 (Computer Fraud and Abuse) for one of the 1998 intrusions. In the plea agreement, Burns also admitted his criminal activity into several other intrusions including the White House website. In November 1999, Burns was sentenced to 15 months in prison, 3 years supervised release and $36,240 in restitution and a $100 fine.

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title 8 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

Mewhiney: Throughout 1996, National Oceanic and Atmospheric Administration (NOAA) suffered several computer intrusions which were also linked to intrusions occurring at the National Aeronautics and Space Administration (NASA). These

computer intrusions continued through 1997. The FBI worked the case jointly with NOAA, NASA, and the Canadian authorities and identified the subject, Jason G. Mewhiney, who resided in Canada. The original damage assessment that Mewhiney had caused, exceeded $40,000. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, Mewhiney pleaded guilty to 12 counts of intrusions which included violations spanning from May 1996 through April 1997, of destroyed/altered data and intrusions with the intent to damage. In the Canadian Superior Court of Justice, Mewhiney was sentenced to 6 months in jail for each of the counts to run concurrently.

Bliss: In February, 1998, the FBI opened an investigation to assist the U.S. Air Force and U.S. Navy regarding multiple computer intrusions. The case was worked jointly with the U.S. Naval Criminal Investigative Service and Florida State Attorney's Office in Jacksonville, FL. The subject was identified as Jesse Le Bliss, a student of the University of North Florida. On August 21, 1998, Bliss pleaded guilty to one felony count for violation of Florida State Statute 815.06 entitled, Offenses Against Computer Users. On September 19, 1998, Bliss was sentenced in the Fourth Judicial Circuit, State of Florida, to six months house arrest followed by three years probation, 200 hours of community service, and a written letter of apology to the Commandant of the United States Marine Corps.

CD Universe: One pending case being worked by the FBI's New Haven Division and the U.S. Secret Service has been widely reported in the press, due to statements made to reporters by the alleged perpetrator. In December 1999, the FBI's New Haven Division opened a case into the intrusions into the computers of CD Universe, an on-line music seller, and the theft of customers' credit card numbers and a related extortion attempt. Because of the credit card aspect, the FBI called the USSS to ask if USSS wanted to investigate jointly. The USSS declined. In January 8, 2000, the New York Times ran a front page story about the case, based on conversations between the reporter and the alleged perpetrator. Subsequently, USSS called the FBI back and requested to work the case jointly. That case is still pending.

OTHER

There are other investigations that are being conducted with other agencies, however further details may adversely impact the investigation due to their pending status. There are currently 47 pending investigative cases which are being worked jointly between the FBI and the multiple entities of the Department of Defense. An additional 58 cases were investigated jointly with other entities that are now in closed status.

RESPONSES OF LOUIS J. FREEH TO QUESTIONS FROM SENATOR DIANNE FEINSTEIN

Question 1. Under Presidential Decision Directive 63 (PDD 63), the * * * [sic * * * NIPC] * * * is supposed to take the lead in warning of, investigating, and responding to threats to or attacks on this country's critical infrastructures. NIPC includes representatives from the FBI and other law enforcement agencies. You testified that the NIPC has improved the FBI's ability to right cybercrime and that the FBI closed 912 cybercrime cases in the Fiscal Year 1999 and had 834 pending cybercrime cases that year.

How many of the 912 closed cases involved threats to or attacks on our nations's critical infrastructures? Were these cases really a threat to our national security? What about the pending cases? How many involved threats to or attacks on our nation's critical infrastructures?

Answer 1. The nation's "critical infrastructure" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems.

This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus, there is no methodology to determine which cases ultimately constitute a threat to our nation's critical infrastructure.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

Question 2. In testimony last February 16, you said that the FBI was producing "fast-developing leads" and that a break in the case was imminent. A couple of weeks later, Michael Vatis, director of NIPC, suggested that in fact agents were making slow progress in the case. How would you assess progress in the case now?

Answer 2. In fact, the testimonies of FBI Director Freeh and NIPC Director Vatis were entirely consistent. Both cited the difficulties in conducting cyber crime investigations, but both also expressed optimism about the prospects for a successful resolution of the case. Director Freeh's February 16 testimony for the record contained the following remarks about the DDOS investigation:

> 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. (Emphases added.)

NIPC Director Vatis' February 29 testimony for the record contained the following statement about the DDOS investigation:

> On February 8, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the tar-

get's log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

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

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

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

Indeed, the FBI's investigation, conducted in close coordination with the Royal. Canadian Mounted Police, very quickly had resulted in the identification of one subject in Canada. Because additional evidence needed to be gathered by the RCMP in the DDOS case and in another matter that came to light during the RCMP's investigation, the subject could not be immediately arrested, and the investigation's progress could not be discussed publicly. However, on April 15, the RCMP executed a search warrant and arrested a juvenile charging him with one of the attacks.

We would therefore assess the progress in this case as substantial and, indeed, unprecedented in a case of this scope and nature. The investigation continues into the attacks on DDOS victims, and we believe good progress continues to be made.

Question 3. In testimony last February 16, you suggested that the FBI's resources "are stretched paper-thin" because of the lack of high-caliber government forensic computer experts. How much has this contributed to the government's lack of success in catching the perpetrators of the February cyber attacks?

Answer 3. As discussed above, substantial progress in fact has been made in the DDOS investigation, with one subject already identified in Canada.

That said, given the explosive growth in computer crimes, our existing resources both in the Computer Analysis Response Team and in the NIPC and the related field office National Infrastructure Protection and Computer Intrusion Program are indeed stretched paper thin.

The Laboratory Division's CART team supports the investigation of any sort of criminal investigation in which evidence might be found on a computer (such as a drug trafficker's accounts) by conducting computer forensic examinations on seized media. The Lab's technically trained agents develop, deploy, and support equipment to perform Title III and FISA interceptions of data communications on the Internet. Staff in both of these areas (forensics and engineering support) is extremely stretched because these agents are tasked with providing support not only for cyber crimes, but all traditional crimes in which digital evidence may be present or data interception required.

The FBI's CART program, consisting of agents and analysts who examine digital medial in order to gather evidence, is not able to keep up with the increasing workload. The following is a summary of current and future trends assuming that the FBI Laboratory is funded for all pending budget requests:

CART Capacity and Backlog

Year	FTE Staffing	Capacity	Exam Requests	Case Backlog	Backlog Time (Months)
1999	95	1900	3500	1600	10.1
2000	104	2080	5000	2920	16.8
2001	154	3080	6000	2920	11.4

CART Capacity and Backlog—Continued

Year	FTE Staffing	Capacity	Exam Requests	Case Backlog	Backlog Time (Months)
2002	213	4260	8500	4240	11.9

In addition, the FBIs Laboratory Division currently provides support not only for FBI cases, but also for the Drug Enforcement Administration and the Immigration and Naturalization Service.

The NIPC and the field office NIPCIP squads are responsible for conducting investigations of cyber attacks, including computer intrusions, viruses, and denials of service. The NIPC currently has 193 FBI Special Agents in the field offices investigating approximately 1200 computer intrusion and other "NIPCIP" cases. Only 16 Field Offices have full squads of seven or more agents. The other field offices have only 1 to 5 agents, who are responsible for not only cyber investigations, but also for industry liaison, the InfraGard Initiative, the Key Asset Initiative, and support to other investigative programs. Further, the NIPC lacks sufficient computer scientists and analysts to support the field office investigations. For instance, it has only 7 network analysts/electrical engineers to support investigations such as DDOS attacks.

The NIPC's and Field Office resources have remained relatively static. The NIPC Headquarters budget for fiscal years 99–01 has been as follows:

Fiscal Year	Budget Authority
1999	29,057,000 (included one-year funding of $10 million for special contingencies in Attorney General's Counter-terrorism Fund)
2000	19,855,000
2001 requested	20,396,000

Meanwhile, our pending case load has grown rapidly.

Fiscal Year	Pending Case Load at End of Fiscal Year
1998	601
1999	801
2000 (as of May 1)	1072

Clearly, then, resources have not kept pace with the crime problem.

Evidence gathering for computer intrusions mandates a prompt response because the digital evidence trail can disappear so quickly. The complexity of documenting, examining and analyzing the tremendous amount of information that is necessarily collected in these types of cases and its very technical nature requires investigators, examiners, and analysts with extremely specific skills and experience. Because of the technical nature of this crime, it is difficult, if not impossible, to temporarily assign additional Special Agents to an investigation since a special technical skill set is required to investigate such matters.

Staff shortages impede not only our ability to conduct investigations adequately, but also to quickly obtain information, conduct analyses, and craft and issue appropriate warnings and alerts. This makes the Indications and Warning mission much more difficult to perform.

Question 4. Some have argued that the high-profile February attacks on Yahoo, eBay, and other companies were just a diversion, allowing the hackers to focus on making smaller, intrusive attacks on smaller sites. Have you found any evidence for this contention?

Answer 4. No. There are individuals and groups who do focus on planning and executing more intrusive attacks, often for the sake of stealing information or money, but we have not seen any correlation between such intrusions and the February DDOS attacks.

Question 5. Why don't you think industry can solve this problem itself?

Answer 5. The Internet was not designed with security as the foremost consideration. Moreover, until very recently, security was not a major priority of either hard-

ware/software manufacturers or consumers. As a result, networks are still rife with vulnerabilities. Improving security on the Internet is thus first and foremost the responsibility of industry. Government must protect its own systems, and can assist industry by providing information about threats and vulnerabilities that we are aware of, and the NIPC does that. But it is industry's responsibility to secure privately owned systems.

Even if systems were more secure, however, there would inevitably be some amount of computer crime committed on the Internet—including not just intrusions, denials of service, and viruses, but also traditional crimes perpetrated over the Internet such as fraud and dissemination of child pornography. As long as crime exists, the public will expect law enforcement to investigate and apprehend the perpetrators. And effective law enforcement is a key element in any strategy to deter further criminal activity. Thus, industry and law enforcement must work closely together.

Question 6. How big a problem is this for the FBI? Do you believe that there are important cyber attacks that are never investigated by law enforcement because the attacked companies refuse to report them?

Answer 6. The vulnerabilities that permeate the industry are a big problem for the FBI and other law enforcement agencies because they make it so easy for crimes to be committed. This accounts in part for the tremendous growth in our case load. For us to be able adequately to address this still growing crime problem, our resources must keep pace. Otherwise, we will not be able to meet the public's demand for effective law enforcement online.

It is impossible to know how many cases have not been reported by companies. We do believe, however, that our outreach efforts are resulting in greater trust by industry in law enforcement's ability to successfully investigate cases while preserving confidentiality and allowing continued business operations. This, in turn, leads more companies to report incidents to law enforcement. We continue to work hard at building that trust, which is critical to our ability to address the crime problem.

Question 6a. How much cooperation do you get from industry? What can Congress do to improve cooperation and coordination between industry and, law enforcement?

Answer 6a. As discussed above, we are making substantial progress in our relations with industry. Despite the oft-repeated remarks of "security experts" in the media, who are interested in having companies report to them instead of to law enforcement, more and more companies are reporting incidents to the FBI. The good cooperation we received from DDOS victims in February is a good example of this. One reason why this cooperation is not well known is that the FBI maintains the confidentiality of those who desire it. The FBI is also building its InfraGard program to promote dialogue and cooperation among industry players and between industry and the government. These chapters are based around the FBI field offices. Congress can best support these endeavors by providing the resources necessary to support and expand our various initiatives.

Question 6b. Do you support a FOLA exemption for industry?

Answer 6b. The FBI has been informed by many in industry that they fear that FOIA does not provide the clear, concise and explicit protection from disclosure of information they might provide to the government relative to cybercrime incidents. The FBI's review of both the statute and its case law interpretation supports the reasonable belief that existing FOIA provisions do provide some significant protections against disclosure of such information such as data which is classified in the interests of national security, information compiled for law enforcement purposes and commercial proprietary information voluntarily submitted to the government by industry with the expectation that it remain confidential. Still, it must be acknowledged that, if the objective is to encourage increased information sharing between the private and public sectors, perception may be more important than reality. For this reason alone, the FBI favors clarifying FOIA law to any extent necessary to provide industry with the confidence it needs to encourage its voluntarily disclosure of critical infrastructure information to federal, state and local governments.

RESPONSES OF LOUIS J. FREEH TO QUESTIONS FROM SENATOR CHARLES E. GRASSLEY

Question 1. Of the 800 cases referred for criminal investigation in fiscal year 1999 from the NIPC, what percentage of these cases were referred to other agencies, other than the FBI, for continued investigation and possible criminal prosecution?

Answer 1. As a general matter, the NIPC does not "refer" cases. Cases are normally initiated by a field office, whether a Field Office of the FBI, the Secret Service, another federal agency, or a state or local law enforcement agency. NIPC is the

"program manager" of the FBI's computer intrusion investigative program, and so receives information about cases directly from the FBI Field Offices. Under PDD 63, other agencies are also supposed to report information about cyber incidents to the NIPC. Sometimes, NIPC will receive the first report of a cyber incident from a private company, a government agency, or another source, and contact the appropriate FBI Field Office. If another agency has concurrent investigative jurisdiction or some other non-investigative interest, that agency will also be contacted (either by the FBI Field Office of the NIPC). Where joint jurisdiction exists, the FBI field office may work jointly with the relevant other agencies (as discussed further below).

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

There have been, however, several instances in which the NIPC or an FBI field office has contacted another agency to determine if that agency wanted to conduct an investigation either jointly or separately, but that agency declined. A couple of examples are listed below.

In May 2000, the FBI's Detroit Field Office referred a complaint to the local Secret Service office regarding a denial of service attack against NHL.com, going so far as to transfer the call from the FBI field office to the Secret Service field office. The Secret Service told the complainant that no one was in the office to receive the complaint due to a visit of Texas Governor George W. Bush to Michigan. The complainant then called the FBI again and the Detroit Field Office took the complaint and assigned the matter for investigation.

Also in May 2000, based on FBI source information, the NIPC notified the USSS headquarters that there may be a vulnerability with the White House Webpage that gave the public access to all the files on that server. The USSS advised that the system administrator may already be aware of this. Neither the NIPC nor the FBI's Washington Field Office has heard back from the USSS regarding this matter.

In another instance, the FBI's Williamsport, Resident Agency, part of the Philadelphia Field Office, opened an investigation into a series of computer intrusion into 10 companies resulting in the loss of approximately 28,000 credit card numbers. During the initial investigation, the FBI discovered that one of the victims located in Buffalo, NY, had contacted the Secret Service and the USSS had opened a case pertaining to the intrusion against the single victim company, but was not investigating the larger set of thefts. The FBI contacted the Secret Service Division in Buffalo, NY to coordinate the case, since USSS already had a pending investigation. The FBI was told that due to the Security Detail Duties for the First Lady, the USSS would be unable to coordinate at the present time with the FBI on the case.

In addition, the FBI has worked, and continues to work, many investigations jointly with other agencies. Two notable examples include Solar Sunrise and Moonlight Maze. Both cases involved extensive intrusions into Department of Defense and other government agency computer networks. The investigations involved an NIPC-coordinated investigation involving numerous law enforcement, intelligence, and defense agencies, as well as foreign law enforcement agencies.

Beyond those examples, the following are other instances of joint investigations.

DDOS: Numerous Internet commerce sites have been victimized by DDOS attacks since February 7, 2000. These DDOS attacks prevented the victims from offering their web services on the Internet to legitimate users. A DDOS attack uses compromised computer networks to "flood" a victim's computer network with massive amounts of data, which causes the victim's computer network to become overwhelmed and to stop operating. The DDOS attack investigation are investigations in seven FBI field offices, five overseas Legal Attache offices, other government agencies such as NASA, as well as the Royal Canadian Mounted Police. Reflecting the extraordinary level of cooperation on these investigations, on April 15, 2000, the Canadian officials arrested a juvenile charging him with one of the attacks.

Curador: On March 1, 2000, a computer hacker using the name, "Curador", allegedly compromised multiple E-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers. Thousands of credit card numbers and expiration dates were posted to various Internet websites. On March 9, 2000, InternetNews reported that Curador stated, "Law enforcement couldn't hack their way out of a wet paper bag. They're people who get paid to do nothing. They never actually catch anybody." After an extensive international investigation, on March 23, 2000, the FBI assisted the Dyfed

Powys (UK) Police Service in a search at the residence of Curador; Curador, age 18, was arrested in the UK, along with an apparent co-conspirator under the Computer Misuse Act 1990. Under United Kingdom law, both males have been dealt with as adults. Loss estimates are still being determined.

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Burns: In August 1998, the FBI initiated an investigation on an individual only known as "zyklon," who conducted numerous computer intrusions to various computer systems causing damages to websites and system files. The case was worked in cooperation with the Virginia State Police. The investigation identified zyklon to be Eric Burns of Shoreline, Washington. In February 1999, following an execution of a search warrant, Burns confessed to the intrusions. In May 1999, Burns also gained unauthorized access and defaced the webpage for the White House website. At that point the FBI began working with the U.S. Secret Service on the case. In September 1999, Burns pleaded guilty to one count for violation of Title 18 USC Section 1030 (Computer Fraud and Abuse) for one of the 1998 intrusions. In the plea agreement, Burns also admitted his criminal activity into several other intrusions including the White House website. In November 1999, Burns was sentenced to 15 months in prison, 3 years supervised release and $36,240 in restitution and a $100 fine.

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title 18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

Mewhiney: Throughout 1996, National Oceanic and Atmospheric Administration (NOAA) suffered several computer intrusions which were also linked to intrusions occurring at the National Aeronautics and Space Administration (NASA). These computer intrusions continued through 1997. The FBI worked the case jointly with NOAA, NASA, and the Canadian authorities and identified the subject, Jason G. Mewhiney, who resided in Canada. The original damage assessment that Mewhiney had caused, exceeded $40,000. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, Mewhiney pleaded guilty to 12 counts of intrusions which included violations spanning from May 1996 through April 1997, of destroyed/altered data and intrusions with the intent to damage. In the Canadian Superior Court of Justice, Mewhiney was sentenced to 6 months in jail for each of the counts to run concurrently.

Bliss: In February, 1998, the FBI opened an investigation to assist the U.S. Air Force and U.S. Navy regarding multiple computer intrusions. The case was worked jointly with the U.S. Naval Criminal Investigative Service and Florida State Attorney's Office in Jacksonville, FL. The subject was identified as Jesse Le Bliss, a student of the University of North Florida. On August 21, 1998, Bliss pleaded guilty to one felony count for violation of Florida State Statute 815.06 entitled, Offenses Against Computer Users. On September 19, 1998, Bliss was sentenced in the Fourth Judicial Circuit, State of Florida, to six months house arrest followed by three years probation, 200 hours of community service, and a written letter of apology to the Commandant of the United States Marine Corps.

CD Universe: One pending case being worked by the FBI's New Haven Division and the U.S. Secret Service has been widely reported in the press, due to statements made to reporters by the alleged perpetrator. In December 1999, the FBI's New Haven Division opened a case into intrusions into the computers of CD Universe, an on-line music seller, and the theft of customers' credit card numbers and a related extortion threat. Because of the credit card aspect, the FBI called the USSS to

ask if USSS wanted to investigate jointly. The USSS declined. In January 2000, the New York Times ran a front page story about the case, based on conversations between the reporter and the alleged perpetrator. Subsequently, USSS called the FBI back and requested to work the case jointly. That case is still pending.

OTHER

There are other investigations that are being conducted with other agencies, however further details may adversely impact the investigation due to their pending status. There are currently 47 pending investigative cases which are being worked jointly between the FBI and the multiple entities of the Department of Defense. An additional 58 cases were investigated jointly with other entities that are now in closed status.

Question 2. If some of the referred cases are potential violations that are traditionally enforced and investigated by other agencies, please describe your mechanisms and procedures that allow for cyber investigations to be conducted by those particular law enforcement agencies (other than the FBI).

Answer 2. The primary statute used by the FBI in computer intrusion investigations is Title 18, USC, 1030. Under this statute, the FBI has broad authority to investigate computer crime offenses. In instances where the computer crime does not meet FBI jurisdiction, the local FBI field office will refer the complainant to the appropriate law enforcement agency (federal, state, or local) which has authority to conduct the investigation. On other occasions, the FBI may continue to work a matter jointly with another law enforcement agency, even if they do not have primary jurisdiction, to provide needed resources and technical expertise. FBI field offices develop liaison contacts with state and local agencies investigating similar violations under state statutes and complaints are disseminated through these liaison contacts. The above cited credit card case is an example of how the FBI field offices make direct contact with their counterpart field offices, such as US Secret Service, to coordinate aspects of an investigation.

Question 3. Please specifically cite the number of NIPC referred cases that have a direct impact or posed a threat on the nation's critical infrastructures.

Answer 3. The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus, there is no methodology to determine which cases ultimately involve a threat to our nation's critical infrastructure.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

Question 4. Please describe the job description and agency of any state and local law enforcement officials currently assigned to NIPC on a full time basis at FBI Headquarters.

Answer 4. The FBI currently has one local law enforcement officer assigned to the NIPC. He is from the Tuscaloosa County Sheriffs Department and his principal job is to work on outreach initiatives to state and local law enforcement as part of the FBI'S responsibility as the "Lead Agency" to work with the "Emergency Law Enforcement Services Sector" under PDD–63. He has also participated in the delivery of training to field investigators under our Key Asset Initiative. This representative replaced an earlier representative from the Oregon State Police, who rotated back to his home agency. The NIPC is also in discussions with several Washington, D.C. area police departments about having officers detailed to the NIPC on a full- or part-time basis.

Question 5. Please describe any private sector representatives, past or present, who voluntarily participate in the Center to facilitate sharing of information between NIPC and the private infrastructure owners and operators.

Answer 5. The NIPC works on a daily basis with private sector representatives to share information. This occurs through such initiatives as InfraGard, which provides information to infrastructure owners and operators on a daily basis, and the pilot project for Indications and Warning that the NIPC has established with the electrical power sector under the auspices of NERC, and the Key Asset Initiative. It also occurs on a case by case basis as we disseminate targeted or general alerts or warnings to industry. The NIPC also works closely with private sector contractors who assist with technical analysis and information sharing.

In addition, the NIPC is working with the Information Technology Association of America to bring private sector representatives into the Center for a period of time as "detailees." That is part of a cybercrime initiative sponsored by the ITAA and the Attorney General.

Question 6. Please describe any private sector representatives that are hired and paid by NIPC funds.

Answer 6. The NIPC has hired contractors to support our work in analyzing cyber intrusions into the infrastructures as well as to provide technical support to our investigations. In addition, a representative from Sandia National Laboratories, has been working at the Center. The NIPC has been reimbursing the Department of Energy under the Interagency Personnel Act for the cost of this detailee's contract.

Question 7. On page 16 of your written testimony, you state: "the FBI, on behalf of the law enforcement community should enhance its technical capabilities (encrypted evidence)." Shouldn't all law enforcement agencies, from federal to state require this capability to accomplish the NIPC mission?

Answer 7. As noted on page 16 of the written testimony, the law enforcement community is extremely concerned about the serious public safety threat posed by the proliferation and use of strong, commercially-available encryption products that do not allow for law enforcement access to the plaintext of encrypted, criminally-related evidence obtained through court-authorized electronic surveillance and/or search and seizure. The potential use of such non-recoverable encryption products by a vast array of criminals and terrorists to conceal their criminally-related communications and/or electronically stored information poses an extremely serious threat to public safety and national security.

In order to address this serious threat and as noted in the written testimony, it is imperative that law enforcement enhance it technical capabilities in the area of plaintext access to encrypted evidence. As part of the government's approach to the encryption issue, the Administration has expressed support for and has proposed the creation of a law enforcement Technical Support Center within the FBI for the purpose of providing the entire law enforcement community with urgently needed plaintext access technical capabilities necessary to fulfill its investigative responsibilities in light of the proliferation of strong, commercially-available encryption products within the U.S. In fact, included in the Administration's Cyberspace Electronic Security Act of 1999 which was forwarded to the Congress last September is a provision that authorizes to be appropriated $80 million to the FBI for the creation of the Technical Support Center, which will serve as a centralized technical resource for federal, state and local law enforcement in responding to the ever increasing use of encryption by subjects of criminal cases.

The TSC is envisioned as an expansion of the FBI's Engineering Research Facility (ERF) to take advantage of ERFs existing institutional and technical expertise in this area. This approach represents a cost effective, non-duplicative and efficient means of provide every U.S. law enforcement agency with access to technical capabilities needed to address lawfully seized encrypted evidence and is supported by the International Association of Chiefs of Police, the National Sheriffs Association and the National District Attorney Association as well as the Information technology industry.

Question 8. Please describe which agencies were in the past participating in the NIPC, but are no longer members. Describe the reasons given by those agencies to the FBI for their withdrawal from participation.

Answer 8. One of the difficulties in attempting to operate an interagency Center is ensuring that all relevant agencies participate. Agencies have not received direct funding to participate in the Center, and so must take detailees to the NIPC out of existing personnel resources. In addition, personnel with cyber expertise are unfortunately in very short supply, meaning that agencies must commit to take scarce resources and send them outside their agencies. Despite these impediments, numerous agencies have sent detailees to the NIPC, including: Defense/Office of the Secretary of Defense; Central Intelligence Agency; National Security Agency; Air Force Office of Special Investigations; U.S. Navy; U.S. Army; U.S. Postal Service; Defense Criminal investigative Service; General Services Administration; U.S. Air Intelligence Agency; Department of Commerce, and the Tuscaloosa, AL Sheriff's office. In addition, we have foreign liaison representatives from two allied countries who assist in coordinating international activities with our counterparts. A representative from FAA is also scheduled to start at the end of June. Additional representative from DoD, CIA, and NSA are also slated to arrive in the near future. We are also expecting representatives from local Washington area police departments on a part-time basis.

Some agencies were represented earlier but do not currently have representatives. Circumstances necessitated the recall of the first State Department representative. State agreed to do so, and has committed to NIPC that it would replace him with two new representatives. DoE's first representative rotated back after more than two years. NIPC's understanding as to why this representative rotated back is that he was at NIPC for a lengthy time and was needed at DoE headquarters to assist in a DOE reorganization. DoE has committed to replacing that detailee.

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has not yet committed to replacing them. Secret Service has not provided any written explanation for this, but in oral discussions, Secret Service officials stated that USSS was not getting additional funding for its electronic crimes program despite its participation in NIPC; the FBI was receiving more media attention in the cyber crime area; and NIPC had not "referred" cases to Secret Service for investigation. NIPC offered any support it could give to Secret Service in addressing budget requests; noted that NIPC public statements often referred to partnership with USSS; and offered to do more to support USSS initiatives with public statements and case analyses. NIPC also stated (as discussed further below) that its role is not to create and "refer" cases; rather, cases generally originate in Field Offices, and FBI and Secret Service field offices frequently work computer crime cases together.

NIPC fully recognizes the value other agencies bring to the cyber crime and infrastructure protection mission. That is why NIPC is an interagency Center, and has senior managers from other agencies in addition to investigators and analysts. For instance, the NIPC Deputy Director is from DoD/OSD; the Section Chief of the Analysis and Warning Section is from CIA; the Assistant Section Chief of the Computer Investigations and Operations Section is from Air Force OSI; the Unit Chief of the Analysis and Information Sharing Unit is from NSA; and the Unit Chief of the Watch and Warning Unit is from the U.S. Navy. Secret Service formally occupied the position of Assistant Section Chief of the Training, Outreach, and Strategy Section. Recognition of the need for other agency participation is also what drives NIPC to continually seek additional representatives from other agencies. It is also reflected in the numerous joint investigations that NIPC and FBI Field Offices have been involved in with other agencies (as discussed further below).

RESPONSES OF LOUIS J. FREEH TO QUESTION FROM SENATOR PATRICK J. LEAHY

Question 1. Can an attempt to commit a violation of 18 U.S.C. § 1030 (a)(5) currently be prosecuted under the attempt provision found in 18 U.S.C. § 1030(b), even if the attempt does not result in loss of at least $5,000 or cause one of the other results listed in § 1030 (e)(8)?

Answer 1. The question calls for an answer interpreting prosecution authority under statute, and as such, is more appropriately propounded to the Department of Justice. As a general rule, however, the FBI understands that, under certain factual circumstances, 18 U.S.C. § 1030(b) does allow for the prosecution of violations of 18 U.S.C. § 1030(a)(5) even if the attempt does not result in a loss of at least $5,000 where evidence demonstrates the offender's specific intent was to cause a loss in excess of $5,000.

Question 2. If an attempt cannot be so prosecuted, would amending the statute so that the aggravating factors included in the definition of "damage" in 18 U.S.C. §§1030 (e)(8)(A)–(D) are instead moved to be elements of the offense under §1030 (a)(5) change that result?

Answer 2. The question calls for a hypothetical interpretation of a statutory amendment as applied through the substantive case law of "attempt," and should be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI does not understand that elevating the definitional elements of the term "damage" to become substantive elements of section 1030 offenses will, in all circumstances, resolve the attempted offense issues generated by the facts of most investigations. Instead, the FBI favors an approach which would combine a restructuring of the elements of the definition of "damage" into the penalty provisions of section 1030(c) with the creation of a lesser offense for those circumstances where damages of $5,000 or more cannot be substantiated. The FBI believes that some unauthorized access intrusions into computers affecting interstate commerce (i.e., protected computers) are so inherently violative as to justify Federal criminal sanctions even where there is no change affecting the integrity or availability of data or where the actual damages suffered do not attain the $5,000 threshold. The intentional unauthorized computer intrusion into the privileged and private medical records of citizens is but one such example. Such a statutory approach as has been suggested by DoJ's Computer Crime and Intellectual Property Section (CCIPS) would create a lesser included misdemeanor offense where the $5,000 threshold is not, in fact, demonstrated and would provide jurors in cases involving damages close to the threshold a legitimate alternative for otherwise violative behavior.

Question 3. If a definition of "loss" were added to §1030(e) to define loss as "the reasonable cost to any victim of responding to the offense, conducting a damage assessment, restoring data, programs, systems or information to their condition prior to the offense and any revenue lost or costs incurred by the victim as a result of interruption of service," would the $5,000 threshold be easier to meet than under current law?

Answer 3. The FBI favors any amendments which allow for the increased inclusion of any costs, losses or other expenditures that a victim would not have reasonably incurred but for the violation regardless of whether those losses resulted from an actual interruption of service. The FBI favors such a definition which would also include, if reasonable, the cost of system reconfiguration related to deterring or eliminating similar future violations.

Question 4. With respect to violations of §1030(a)(5)(A), is it your understanding that each separate "transmission" could form the basis of a separate count? Similarly, with respect to violations of §§1030(a)(5) (B)–(C), is it your understanding that each separate "intentional access[] could form the basis of a separate count?

Answer 4. The question calls for an interpretation of a statute applying the substantive case law of what constitutes "criminal episode," and related concepts of what constitutes appropriate "joinder," or "severance" under the Federal Rules of Criminal Procedure and should more appropriately be directed to the Department of Justice for a detailed and definitive response. As a general matter, however, the FBI understands that whether a single computer transmission of malicious code under section 1030(a)(5) may form the basis for a single count under an indictment will, in large measure, turn upon the unique facts of any given investigation. Whether a single transmission of a self-replicating, self transmitting destructive computer virus constitutes one transmission, and therefore one count or thousands of transmissions intentionally effectuated by chain reaction, and therefore thousands of counts, may turn upon an evaluation of numerous factors not the least of which would include the object and intent of the offender/transmitter, the design of the code, the reasonable foreseeability of re-transmission and, as a practical matter, the ability to track, gauge and prove the re-transmission. Similarly, whether, in a computer network environment, the repeated unauthorized accessing of a computer in violation of section 1030(a)(5) (B)–(C), which accessing is temporally related, will, as a practical matter, frequently turn upon the configuration of the network and its security and banner system, to name but a few factors.

Question 5. Are you aware of any cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. §1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. §5G1.2, which provide that sentences on multiple counts may be imposed consecutively to the extent necessary to produce a combined sentence equal to the total punishment called for by the guidelines?

Answer 5. The NIPC referred this question to the Department of Justice Computer Crimes and Intellectual Property Section for input. The Department reported that it could recall no cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. § 1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. § 5GI.2.

Question 6. Please explain the reason, if any, to continue the codification of the work-sharing agreement between the Secret Service and the Federal Bureau of Investigation found in § 1030(d)?

Answer 6. In 1996, Congress specifically limited the Secret Service's authority to investigate crimes under 18 U.S.C. § 1030 to those offenses under subsections (a)(2)(A) and (B), (a)(3), (a)(4), (a)(5) and (a)(6). The Senate Report accompanying the 1996 amendment explained that:

> [t]he new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

S. Rep. No. 357, 104th Cong., 2d Sess. 13 (1996).

Inherent in the 1996 changes was the recognition that the statute was being amended to reflect the respective investigative jurisdictional limits existing at that time. It was clear at that time that the jurisdiction of the Secret Service, found at 18 U.S.C. § 3056, did not encompass the types of offenses described in Section 1030 (a)(1), (a)(2)(C), or (a)(7).[1] Given that there have been no additional grants of general investigative jurisdiction to the USSS since that amendment, it is not clear why the USSS's jurisdiction over computer crimes under Section 1030 should be expanded. The theft of National Security information which is the type of information Section 1030(a)(1) was intended to address has never been the subject of USSS jurisdiction. In addition, the types of crimes contemplated by 1030 (a)(2)(C) and (a)(7), as recognized by the legislative history, have traditionally been investigations solely in the province and expertise of the FBI.

The 1996 provision is an explicit effort by Congress to address the criminal offenses at issue through a division of labor primarily determined by investigative responsibility and expertise. Any reversion to the pre-1996 jurisdictional provisions raises serious issues and concerns about the utilization of resources and proper coordination. Concurrent jurisdiction would result in a duplication of efforts that would waste resources and encourage independent investigations by separate agencies at the expense of coordinated joint efforts. Indeed, given the decision by Secret Service to refrain from participation in the National Infrastructure Protection Center (NIPC) (both by detailing personnel and providing investigative information from its cases) despite a mandate from the President to do so under PDD–63, expanding USSS's cyber jurisdiction at this time would result in a fractured approach to sensitive intrusion investigations involving espionage, extortion, and other serious matters.

Question 7. The FBI has limited authority to issue administrative subpoenas in certain cases, such as federal health care fraud or sexual exploitation or other abuse of children. Since cybercrime cases are criminal in nature, is the FBI able to obtain documents relevant to the investigation with grand jury subpoena? To the extent that documents obtained with a grand jury subpoena need to be shared with third-party experts, can permission be obtained to do so under Federal Rule of Criminal Procedure 6(e)(3)?

---

[1] "Under the direction of the Secretary of the Treasury, the Secret Service is authorized to detect and arrest any person who violates—

(1) section 508, 509, 510, 871, or 879 of this title or, with respect to the Federal Deposit Insurance Corporation, Federal land banks, and Federal land bank associations, section 213, 216, 433, 493, 657, 709, 1006, 1007, 1011, 1013, 1014, 1907, or 1909 of this title;

(2) any of the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; or

(3) any of the laws of the United States relating to electronic fund transfer frauds, credit and debit card frauds, and false identification documents or devices; except that the authority conferred by this paragraph shall be exercised subject to the agreement of the Attorney General and the Secretary of the Treasury and shall not affect the authority of any other Federal law enforcement agency with respect to those laws.

Answer 7. Generally speaking, a "governmental entity" is authorized under 18 U.S.C. 2703(b)(1)(B) to obtain the contents of an electronic communication in remote computer storage with prior notice, as delimited in 18 U.S.C. 2703(b)(2), by using an administrative or grand jury subpoena. A governmental entity is also authorized under 18 U.S.C. 2703(c)(1)(C) to obtain certain subscriber or customer information from a provider of electronic communication services or remote computing service, by using an administrative, grand jury, or trial subpoena, or as otherwise permitted under 18 U.S.C. 2703(c)(1)(B). The Electronic Communications Privacy Act (ECPA) does not itself identify which federal agencies qualify as "government entities" authorized to issue administrative subpoenas. Currently, the FBI is authorized to issue administrative subpoenas in cases involving health care fraud under 18 U.S.C. § 3486 and in cases involving child pornography and sexual solicitation under 18 U.S.C. § 3486A. Unfortunately, there does not currently exist a statute authorizing or designating the FBI as a "governmental entity" authorized to issue administrative subpoenas for violations of 18 U.S.C. § 1030 or other crimes of fraud increasingly committed by or facilitated through the use of a computer. The absence of such a statute impedes FBI efforts to accelerate an effective response to cyber crime.

While helpful, the use of grand jury subpoena to acquire minimally intrusive transactional information (e.g., so-called "header information" such as "to" or "from") or subscriber information (e.g., the name and address of the owner of an Internet screen name) is frequently a cumbersome and time consuming process especially in investigations where time is of the essence or where the information sought is from an unusually large number of providers. Some circumstances may dictate seeking express court authorization under the provisions of Federal Rule of Criminal Procedure 6(e)(3)(C) for disclosure to non-government experts who may not qualify as personnel assisting the attorney for the government in the investigation before the grand jury. In many cases, the practical concerns of delay and coordination with other agencies and courts further stymies government's ability to provide a timely response to imminent criminal behavior.

The FBI supports an expansion of its statutory authority to issue administrative subpoena under the Electronic Communications Privacy Act for any violation of law within the FBI's existing criminal investigative jurisdiction. The FBI's experience to date in the issuance of administrative subpoena in the areas of health care fraud and child exploitation crimes demonstrates that it can responsibly limit and control the exercise of this authority.

Question 8. Denial of service attacks are increasing exponentially. According to the FBI, these attacks involve the placement of tools such [as] Trinoo, Tribal Flood net, TFN2K or Stechenldraht on unwitting victim systems, which then send messages upon remote command to a targeted computer system until that system is overwhelmed and essentially shut[s] down. In order to document in real-time the remote command being given and the triggering of the message flood to the target system, is law enforcement currently required to obtain a wiretap order since the unwitting victim system is not a "party to the communication" authorized to grant consent to electronic surveillance? Would an exception to the wiretap law to allow the unwitting victim system operator to grant consent to electronic surveillance be helpful to law enforcement?

Answer 8. The question calls for an interpretation of a statute which would more appropriately be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI understands that:

(1) the provisions of 18 U.S.C. § 2511(1)(a) prohibit all interceptions unless expressly authorized elsewhere in the Act;
(2) the provisions of 18 U.S.C. § 2511(2)(a)(i) authorize a provider of wire or electronic communication services to intercept communications on their system, not because they are parties to those communications, but as "is a necessary incident to the rendition of [that] service or to the protection of the rights or property of the provider * * *;"
(3) many providers (especially start-up Internet services) may not have the necessary tools or expertise to adequately track, document or halt an intruder in their system and, more perhaps more significantly, no providers have compulsory process to facilitate disclosure of transaction and subscriber information from other providers which is necessary to identify the source of an attack;
(4) 18 U.S.C. § 2511(2)(a)(i) does not permit law enforcement to conduct an interception (without a court order) even upon a provider's express request when the provider's system has been invaded or trespassed upon by a hacker, and
(5) as a result of this quandary, and in order to ensure that evidence obtained will subsequently be held admissible, law enforcement is required to obtain a court order in order to enable it to actively work in conjunction with the provider.

Given the high level DOJ approval that is required for Title III Interception applications, the necessary generation of paperwork, and the time needed by the reviewing court, significant delay can occur before law enforcement can provide an effective response to a hacker or DDOS event. This anomaly in the law creates an untenable situation whereby providers are sometimes forced to sit idly by as they witness hackers enter and, in some situations, destroy or damage their systems and networks while law enforcement begins the detailed process of seeking court authorization to assist them. In the real world, the situation is akin to a homeowner being forced to helplessly watch a burglar or vandal while police seek a search warrant to enter the dwelling. For these reasons, the FBI favors enactment of a statutory exception under 18 U.S.C. § 2511 which would expressly authorize law enforcement to assist such providers by intercepting the communications of a computer user/trespasser (the transmissions to and from the user/trespasser) BUT ONLY upon the voluntary, written consent of a service provider after that provider has made an initial determination that the user/trespasser is, in fact, not authorized to be on the system or network. Such an exception to the general interception prohibition would accelerate exponentially law enforcement's ability to respond to such hacker incidents and would be a significant step toward ensuring the security and integrity of the Nation's critical infrastructure.

Question 8a. Is law enforcement currently required to obtain a wiretap in order to document in realtime the remote commands being given to a target system?

Answer 8a. Although the FBI respectfully refers questions of statutory construction to the Department of Justice, the federal code at 18 U.S.C. 2511(2)(b) states that "a person or entity providing electronic communication service to the public may divulge the contents of any such communication * * * which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." In that manner, it is possible for law enforcement, without a wiretap order, to obtain from a service provider remote commands, documented in realtime, that appear to pertain to the commission of a crime. Another manner in which law enforcement, without a wiretap order, might obtain in realtime the remote commands being given to a target system is pursuant to the consent provision of the federal code, 18 U.S.C. 2511(2)(a), which permits "a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." Many target systems include banners warning that use of the system depends on a person's consent to all of their activities being monitored, recorded and/or disseminated at the discretion of the systems administrator, to include if appropriate direct monitoring by law enforcement.

Question 8b. Would an exception to the wiretap law allowing victim system admins to grant consent be helpful to law enforcement?

Answer 8b. The FBI believes that it would be helpful to law enforcement to add an exception to the wiretap law to allow the unwitting victim system operator to grant consent to electronic surveillance for the limited purpose of monitoring a computer trespasser.

Question 9. The Department of Justice objected to the Clone Pager Authorization Act, which passed the Senate in the last Congress, on grounds that clone numeric pagers "obtain all of the information transmitted after a phone call is connected to the called party * * * in the form of electronic impulses. * * * These electronic impulses are the "contents" of the call: They are not used to direct or process the call, but instead convey certain messages to the recipient." For this reason, the Department advised Chairman Henry Hyde, by letter dated May 20, 1998, that capturing the messages transmitted by clone numeric pagers implicated Fourth Amendment and privacy interests.

Do pen register devices capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party?

Answer 9. Law enforcements pen register devices (or dialed number recorders) utilized with regard to telephony services do capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party. (A potential exception to this would be certain pen register-based approaches employed by service providers in switch-based solutions, where post-cut-through dialing (including post-cut-through signaling) may not be provided to law enforcement. This circumstance is currently a subject of review by the FCC under rule making implementing CALEA, and regarding which we anticipate a resolution in the near future.) The distinction between a pen register device on a telephony service and a clone pager (or pager inter-

ception) is that a pen register is employed to capture dialed numbers which are used to set up a call. Hence, in the overwhelming majority of instances where pen registers are used the information captured is simply signaling information used to set up a call. By comparison, pager interceptions are employed to capture the information received by a pager which, in all instances, constitute the content or message of the call. Consequently, the law has historically distinguished the legal processes required for these two types of acquisitions (i.e., pen register authority vs Title III authority, respectively).

Pen register efforts in the data network area work somewhat differently. The most basic reason for this is because the services (e.g., email, web-based mail, voice over IP) and applications (e.g., Internet Chat, File Transfer) transmitted over data networks are somewhat different. Some of these services and applications lend themselves to precise ways of capturing (i.e., recording) call identifying and signaling information only while others make the process of differentiating signaling information from call content more difficult.

Question 9a. Section 3121(c) of title 18, United States Code, requires government agencies authorized to use pen registers to "use technology reasonably available * * * that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Please describe the technology and methodology currently employed to comply with this statutory requirement.

Answer 9a. Pen Register devices on telephony services continue to operate as they have for decades. Stated differently, since the enactment of CALEA, there has been no change in technology or pen register equipment for telephony that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

As stated above, pen register efforts in the data network area work somewhat differently, and there, where technology that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information is reasonably available, it is employed. For example, the FBI employs pen register devices to capture Internet Protocol (IP) addresses. Since data networks typically use well-established layered protocols, FBI tools are capable of restricting the information captured to the IP address.

Question 10. Section 3121(a) of title 18, United States Code, requires a court to authorize the use of a pen register if the court finds that the government attorney has certified that the information likely to be obtained by "such use is relevant to an ongoing criminal investigation." The certification by the government attorney is, in turn, made under oath and penalty of perjury, under section 3122.

Is the government attorney required to describe to the court in the application for a pen register the factual basis for the attorney's certification that "such use is relevant to an ongoing criminal investigations"?

As a matter of regular practice, do government attorneys or State law enforcement or investigative officers making applications for pen registers describe for the court the factual basis for the certification that "such use is relevant to an ongoing criminal investigation" or does this practice vary?

What procedures, including audits or internal reviews, are in place to ensure that government attorneys and State law enforcement or investigative officers comply with the statutory standard and have the necessary factual basis for making the application, particularly in those districts where the practice in applying for pen register orders is not to describe for the court the factual basis for certification?

Should the court, rather than governmental attorneys or State law enforcement or investigative officers, be given the authority to make the factual finding that "information likely to be obtained by such installation and use [of a pen register] is relevant to an ongoing criminal investigation," and if not, please explain why?

Answer 10. Several of the questions call for or implicate an interpretation of statute which would more appropriately be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI understands the Supreme Court has expressly ruled that "the installation of a pen register * * * [is] not a "search" within the meaning of the Fourth Amendment and therefore its use does not violate the Constitution." *Smith* v. *Maryland*, 442 U.S. 735, 745–46, 99 S.Ct. 2577, 2583 (1979). Given the lack of an expectation of privacy at stake in the limited, non-content information garnered through the use of pen registers, the Courts have held that the limited judicial review role delineated by 18 U.S.C. § 3121 et seq. is Constitutional and is intended to safeguard against the purely random use of pep register devices by ensuring compliance with the statutory requirements established by Congress. See *United States* v. *Hallmark*, 911 F.2d 399, 401–402 (10th Cir. 1990).

Pen Register certifications by government attorneys are drafted and filed by attorneys of the Department of Justice and not, at the Federal 1evel, by Special Agents of the FBI. Questions regarding the substance of such certifications would more appropriately be directed to the Department of Justice for a more definitive response. As a general matter, however, it is the FBI's experience that the degree to which a pen register application to the Court discloses the underlying factual basis for the attorney's certification turns, in large measure, upon the nature of the statutory offense which is the focus of the investigation. Whereas section 3123(b)(1)(D) requires that all pen register orders contain a "statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates," it follows that the application required by section 3122(b)(2) contain such a statement within the attorney's certification and it is the FBI's experience that this is commonly the case. Depending upon the nature of the offense described in the certification, the underlying basis for the certification can, and in most instances will be readily apparent. Thus, in telemarketing fraud investigations, the obvious underlying basis is that the offenders are using the telephone to solicit victims. Similarly in narcotics and conspiracy to commit narcotics violations, the reliable and common sense inference is clearly that telecommunications are being used to facilitate the possession, distribution and sale of controlled substances in violation of Title 21 of the United States Code. Even in investigations involving computer hacking in violation of the Computer Fraud and Abuse Act (18 U. S.C. § § 1030 et seq.), it requires little thought or imagination to understand the underlying basis for the request.

The FBI also understands that the sole basis for obtaining a pen register order is to further a criminal investigation by generating reliable admissible evidence. An attorney who falsely or recklessly certifies an application under oath pursuant to 18 U.S.C. § 3122(b)(2) does so at his/her peril subject to sanction, disbarment and prosecution. Furthermore, an attorney who so falsely certifies such an application has no way of knowing the subsequent course and outcome of the investigation. Frequently, information received from a pen register is consolidated with other investigative information and is submitted in subsequent, more detailed applications to the Court such as search warrant applications or wiretap applications. In the unlikely event that an attorney for the government were to submit a false certification to the court in support of a pen register application, the lack of any nexus between the named subjects of the investigation, the "statement of the offense," and the attorney's certification that the information likely to be obtained from the devise's use is relevant to an ongoing criminal investigation would, in many instances, reveal itself either in subsequent applications to the Court for search warrants or wiretaps, or in discovery incident to prosecution. The dearth of such empirical or anecdotal evidence demonstrating inappropriate or false certification of applications by attorneys for the government demonstrates that the certification obligation is conscientiously fulfilled.

Question 11. You have testified that information theft and financial fraud perpetrated online have caused the most severe financial losses, "put at $68 million and $56 million respectively." In fact, you have identified "use of the Internet for fraudulent purposes" as "one of the most critical challengers facing the FBI and law enforcement in general.: Appreciating this challenge, I have urged that the Congress be careful in considering legislation, such as H.R. 1714, "The Electronic Signatures in Global and National Commerce Act," to ensure that consumers are adequately protected in the online environment. This bill has passed the House of Representatives and is currently the subject of a conference with the Senate.

The National Association of Attorneys General has commented on H.R. 1714, stating that the bills provisions permitting storage of only synopses of documents that "accurately reflect" originals, even where the law otherwise requires retention of original documents, "has the strong potential to negatively impact law enforcement discovery of document." Do you agree and, if not, please explain why?

H.R. 1714 would require that state enactments of the Uniform Electronic Transactions Act (UETA) "be consistent with" the House bill, resulting in federal preemption of any state exemption from the presumption of validity of electronic signatures and transactions that is not authorized in the House bill. The National Association of Attorneys General has opined that this broad federal preemption would "unduly hinder the ability of the states to protect their citizens against consumer fraud." If States are hindered in combating consumer fraud, would the FBI's job in protecting the public from fraudulent online practices be made more difficult?

Answer 11. On its face, the provisions of H.R. 1714 which allow for the electronic storage of contracts, agreements and records are unrelated to earlier provisions of the bill delineating what types of legal documents may be executed by electronic signature. To the extent that Section 101(c)(1)(c) could be interpreted as allowing for the electronic imaging and storage as an electronic record of written contracts or

agreement, the tangible originals of which would otherwise be required by law to be maintained in tangible form, then, there could exist the potential to negatively impact certain law enforcement investigations relating to such documents. At a minimum, the supplanting of tangible originals (otherwise legally required to be maintained in tangible form) with electronic images depicting the originals, when coupled with destruction of the originals, would eliminate or complicate handwritten signature analysis and render null the possibility of recovering fingerprints or other trace evidence from the surface of originals. By the same token, the provisions of section 101(c)(2) which exempt from retention data relating to the communication or receipt of any contract, agreement or record electronically recorded, could, in the context of electronically executed contracts, complicate or eliminate law enforcement efforts in tracing the source of transmission of fraudulent transactions or the location and identity of co-conspirators or even other victims. The continued trend toward electronic, paperless execution of commercial transactions (which is admittedly so critical to the continued evolution and expansion of the Internet) when coupled with (1) the growing ability of criminals to utilize encryption to restrict law enforcement's ability to recover crucial inculpatory evidence, and (2) the absence of any preeminent public key, or private signature verification entity or procedure complicates the efforts of the FBI and state law enforcement to protect the public from online fraud.

SYNOPSES ONLY OF DOCUMENTS CAN NEGATIVELY IMPACT LAW ENFORCEMENT?

The review of complete and accurate records is often necessary in law enforcement's effort to help investigate crime. All records management and retention policies therefore can be said to have an effect on law enforcement, and those policies which do not require that information be maintained, at least in theory, can negatively impact law enforcements discovery of that information.

IF STATES ARE HINDERED * * *

The FBI believes that since States are the primary responders to crime in our country, if the States are hindered in combating consumer fraud, then the FBI's job in protecting the public from fraudulent online practices would be made more difficult.