



UNITED STATES DEPARTMENT OF JUSTICE
KEYNOTE ADDRESS OF THE HONORABLE JANET RENO
ATTORNEY GENERAL OF THE UNITED STATES
AT
THE ITAA CYBERCRIME SUMMIT:
A LAW ENFORCEMENT/IT INDUSTRY DIALOGUE ON
PREVENTION, DETECTION, INVESTIGATION AND COOPERATION

EDS Building

13600 EDS Drive

Auditorium

Herndon, Virginia

Monday, June 19, 2000

P R O C E E D I N G S

ATTORNEY GENERAL RENO: Thank you, Harris Miller, for all that you have done, both in promoting educational opportunities for our young in this area and bringing law enforcement and industry together. And thanks to you, Mr. Brown, and Mr. Dvoranchik, for your hospitality. I think that this is so important that we hold this conference in Northern Virginia where so much innovation is taking place.

I come today to ask you a question. And I look forward to receiving your answers later this afternoon. What can the Department of Justice, what can I as Attorney General do, to build trust and confidence between law enforcement and industry so that we can work together as partners in responding to the growing challenges of cyber crime?

What can we do to meet our obligations to ensure the public safety, to enforce the law, in a manner that fosters and promotes privacy and the civil liberties of all concerned, allows the Internet to flourish with all the innovation that you can muster, and at the same time causes the victim as little inconvenience as possible?

The Department of Justice does not seek in basic government regulation or monitoring of the Internet. We would rather work together as partners with separate but overlapping areas of responsibility and accountability.

The private sector in that regard should take the lead in protecting the security of private sector computer systems. And we should protect government systems. We must share, however, the information about vulnerabilities so that we can each take steps to protect our systems against attack.

have on victims.

But what you will say is, hmm. Have you looked at how the federal government talks? If we give you this information, confidentiality which is so important to us will be ignored. And we will find sensitive information out on the street where we don't need it. Or we will be embarrassed because our lack of security, our lack of prevention, will be made known to the world.

These are issues that we need to address in a candid, frank way to understand just what is involved. The same is true in the non online world. The banker doesn't want to report his embezzlement because he's embarrassed. The banker doesn't want to report the details because it will lead to confidential information that is important to the bank being out in the public. How can we work together to ensure confidentiality?

The next point that you will raise is don't you know how inconvenient and burdensome the criminal justice system is and an investigation is? You're going to have all my employees down before the grand jury. You're going to have them tied up in interviews after interviews. Ah, forget it. I'll protect myself. I don't need you.

Then comes the denial of service attack or other similar situations. And you say, oh, wait a minute. Maybe we do need them. Let's start now to minimize the problems that victims perceive in the criminal justice system.

Then there will be a, okay. You've assured me of confidentiality. But I don't know what's happening. Nobody ever lets me know what's going on and what the next step is. Let us sit down together and help each other understand the two worlds, the worlds of cyber technology and the world of the criminal justice system. Let us try to be candid with you in what we can and can't do.

Then, okay. We got all that done. But after that effort, they just get a tap on the wrist. Nothing happens to them. Let us work together to focus on sentencing guidelines so we get sentences that mean what they say and serve as a deterrent. Let us figure out what we do for that 15 year old hacker that makes sure that he knows never ever to do it again.

But then I hear, look. You're a nice lady. I think your heart's in the right place. But you don't understand. Law enforcement doesn't begin to have the equipment to match wits with the bad guys. And until you get the technology, it's just not going to work and you're not going to be successful. We need you to join with us in letting the world know what is needed in law enforcement to properly protect law enforcement interests that coincide with industry interest.

Harris has alluded to one of its next problems. You say you've got these great people working for you. And as soon as we form a relationship with one, he goes off to the private sector. Then the next one goes off to the private sector. And they're not there long enough ever to establish any contact.

Well, we're trying to develop concepts such as cyber ROTC where we can attract people to government for a longer period of time in return for a system such as ROTC produced. But we have a long way to go. And that goes to educating our young people. How can we look at all of America, not just some of America, and identify -- and Harris, I'm really intrigued with this -- how can we identify young people of 10, 11 and 12 years old who are not do well in school, who are not supervised at home, who do not have motivational or inspirational parents at home, how can we reach out and identify them through aptitude testing that gives us resources that we never thought we had in the United States so that we are not as dependent on the world?

And finally, you will say, but even if we work all this out, we're going to have to extradite somebody. And you'll say, well, we can't extradite because it's a national from another country or because it's too expensive? We need industry to join with us in letting the world know that there is no safe place to hide. And that although borders are meaningless with respect to cyber crime, we have got to effect alliances around the world that will ensure that there are no rogue nations, no rogue jurisdictions, that permit cyber attack around the world.

We've got our work cut out for us. But so do all who have contact with the criminal justice system. There are those that take the challenge -- and I think we should -- for there are those who have used otherwise magnificent tools to really inflict harm on others.

Let us make sure that the Internet is not part of this history. Even in the Internet's relatively short existence, we have seen a dizzying array of the criminal use of the technology. They are not trivial crimes. We have investigated computer attacks on our nation's information infrastructure, including serious breaches in the Department of Defense and NASA in numerous instances in which cyber criminals have stolen credit cards from consumers and posted them on the Internet, not only harms these individuals, but undermines the confidence of the public in the Net.

We must not forget that the Net is being used with increasing frequency to commit traditional crimes, including global distribution of child pornography, fraud schemes, cyber stalking and the like. We have this unprecedented moment.

We have to make sure that we join together now while people are learning about the Net, while they're learning about what can be done and not done on the Net, to know and let them know that there is going to be enforcement. It's an unusual time in history where we can shape the whole public attitude and acceptance of what's right and what's not right.

Just think about it for a moment. It's rare in history that a collection of people, both in law enforcement and in industry, have a chance to say this is the wrong thing to do. This is the right thing to do. These are the sanctions that you face if you do it. We're going to have to be together in that effort.

We have made gains. The Internet fraud Complaints Center provides a centralized repository for filing complaints of Internet fraud. Since it's opening on May the 8th, the center has received an average of approximately 1,200 complaints per week. Through the Center, the FBI and the National White Collar Crime Center, collect, analyze, evaluate and disseminate Internet fraud complaints to the appropriate law enforcement and regulatory agencies.

But that's not going to work if we continue to build complaints, generate backlogs, those backlogs don't get addressed, people don't think anything's going to happen to them, industry loses confidence in law enforcement and it goes from bad to worse.

Yes, we've made some progress, but we've got a long way to go. Senior officials from the Department's Computer Crime Section meet regularly with representatives from Internet providers, telecommunication carriers and others through industry information groups. FBI's National Infrastructure Protection Center and its computer crime squads have worked together to develop the intraguard program in communities around the country.

I think these efforts are critically important, but we've got more to do. We've gathered here today people who I think can address the issue. Each of us has a role to play.

I urge you to talk frankly and openly. Don't be afraid that you will hurt

my feelings or make me mad. I won't get mad and I won't get my feelings hurt except if I don't come out of here with some really specific suggestions about what we can do to be more effective.

Law enforcement like industry has its duties, its tools and its constraints. I want your opinions, your suggestions about what we can do to work in harmony with principles of our constitution and impose the least disruption on your undertakings.

I want you to know that I am not interested in searching people's computers except that we do it the right way. I need your advice in what we do if France is investigating somebody, a French businessman. He's never been out of France. He's got all his records stored in his computer. France gets our equivalent of a search warrant and discovers that he's a customer of America On Line and the records are right over here or over here.

How are we going to deal with those issues? How are we going to deal with the issues of cross state searches? There is so much to be done?

Finally, if you're not interested in working together in just common business good sense because you don't think we can do the job, there is something more important than anything else. It is this nation and all that we hold dear, because of your brilliance, because of your sense of innovation, we are very dependent on cyber technology. We have not kept up with cyber security.

So much of this nation's critical infrastructure, defense, banking, power, emergency services, finance, so much of it is dependent on what you have created. Being dependent, it is also at risk of cyber terrorism.

Let us not wait until we get to the crisis of cyber terrorism before we have learned to work together to solve our problems with lesser crimes. And then, God forbid, that they should come, we will be prepared again and again to prevent whenever possible and to pursue when it has occurred so that these people are brought to justice with a sentence that will serve as a deterrent?

I will be back this afternoon with pen and paper in hand and looking forward to your report. And I am deeply grateful to you all for taking the time today to be with us. It is very important to the Justice Department and to law enforcement.

MR. MILLER: We now have an opportunity for a couple of questions before the Attorney General needs to leave. If you have something written, did people get cards? You should have gotten cards? Oh, in your little packet, you have cards. Actually, if you just want to put your hand up and ask a question. As long as it's on the topic, that will be okay. Nobody has any questions? They've stunned you into silence? We should have planted one in the audience. There's one over there. Yes, sir.

QUESTION: How many (inaudible) or agencies have implemented a complete intrusion detection system, have policies and best practice.

MR. MILLER: The question is how many organizations attending have attending have implemented intrusion, detection and have good solid policies and practices in place?

QUESTION: (inaudible)

MR. MILLER: The first question was kind of a survey of the group. Maybe we'll do that later today. But I think the second question, maybe Dick or the Attorney General wanted to comment. Where if some company or organization were looking for some best practices now, where might they find them? Where would those be available to help a company implement those practices?

MR. BROWN: Well, I don't have a lot of survey data on your question, but I know one company that has. And it works. But, you know, if you look at, for example, EDS, we go through protection and training and operating systems and recovering. A lot of companies don't even know they've been attacked or are state and federal government agencies. They don't know when an attack has occurred and what the residual effect is. So you can work with companies in the IT industries. But then forums, I think, like I referenced in my remarks and have been referenced elsewhere are a gathering point for best practices that we share very freely across the industries of communications and IT and other industries.

ATTORNEY GENERAL RENO: I think if there is not a central place, in many instances law enforcement will go out and do it. We have been careful in this regard because we don't want to be perceived as putting regulations. And we would like to pursue the law enforcement and enforcement side of it. But, Harris, this may be -- you may know better than I do. But if there is not a central place where people can go, perhaps we should be about designing that.

And the other issue that has been raised on a number of occasions, those in the security field know what needs to be done. But sometimes their CEOs need to be advised of what needs to be done and the importance of the effort stressed. We would look forward to working with you in any way that you thought appropriate to address the creation of some central system for understanding the best way to go about it and whatever we can do with CEOs.

MR. MILLER: The ITA has been working with the federal government. We had a meeting last month hosted by the federal CIO council, particularly John Gilligan, who is the Chief Information Officer of the Department of Energy, to talk about best practices. And we brought together industry people as well as senior officials from the government agencies to begin that dialogue. General Reno.

So I think we're going to see that begin to evolve. And the assumption is -- it may turn out to be an incorrect assumption -- is as the federal government develops best practices, those in turn will devolve down to state and local governments and may also migrate into private industry. Obviously, various companies that are specialist information security have their own proprietary methodologies. But whether those are generic enough, we don't know yet.

MR. BROWN: Harris, if I could just also follow-up, and Attorney General Reno mentioned this as well. A lot of companies that I interact with, maybe you do too, there's a conclusion people erroneously jump to that says I'm not sure I've got the best technology to combat this. But more often than not, they do. What's lacking is the policies and the clear thinking about how a business or any organization should apply that technology, the layers of defenses taking advantage of existing technology that needs to be instituted and then the disciplines that people must be expected to adhere to in organizations so that this kind of thing can be thwarted off. And I think that kind of information also if we can have the right forum to share that would be immensely valuable.

MR. MILLER: Thank you, Stuart, last question.

STUART: The Defense Science Board asked me to look at legal issues on the information warfare defense. And one of the tentative conclusions that I think we're coming to is the NIPC can't really effectively deal with the private sector and take into account non law enforcement considerations if it is buried as deep as it is in the FBI. And I wondered what thought had been given to making it more truly inter-agency and getting a higher level of political attention within the government.

MR. MILLER: The question is, I guess primarily to the Attorney General,

whether the National Infrastructure Protection Center, NIPC, is placed in the right position within the government currently which is within the FBI in terms of its ability to deal most effectively with the broad based commercial sector.

ATTORNEY GENERAL RENO: I think it's important because there is no other agency in terms of law enforcement that has the jurisdiction and the authority to make the NIPC's actions real. I think it needs more and more focus as it comes into its own. And I will take back your words.

MR. MILLER: Okay. At this point, General Reno has to leave for another appointment. She will be back this afternoon.

ATTORNEY GENERAL RENO: If anybody has any other questions.

MR. MILLER: Oh, okay. Well, she still wants to stick around. Listen, hey. She's the boss. As long as it's on this topic.

QUESTION: (inaudible) the FBI agent is going to cart away their servers and that's their livelihood if they do make such a report.

ATTORNEY GENERAL RENO: That's the reason we're here today about what's going to be carted away and who's going to be inconvenienced. One of the problems that you face as you prepare a case is developing the evidence sufficient to prosecute. And to develop the evidence, you've got to go through it, make it available to the prosecutor, make it in a form that can be introduced in court.

And what I think we have done is address the issue of just what you're talking about by figuring out what we can do to preserve records, how we can make copies, how we can continue the business without interruption in every way that is possible. And what we have again discovered is that industry often times has some very good ideas about how it can be done.

MR. MILLER: Jim, last question. Oh, there's one more back there. Jim and then the gentleman back there.

JIM: I have also a question for the Attorney General (inaudible). Michael Dell, founder and President, CEO of Dell Computers, spoke at the National Press Club a couple of weeks ago. He made a very interesting statement and I'll just paraphrase. He said Americans can have privacy -- cyber privacy -- or they can have cyber security, but they can't have both. He said the two ideals are in conflict with each other. Do you agree with that?

ATTORNEY GENERAL RENO: I think you have hit upon the great balancing act of this extraordinary document that we live under, how you can have freedom of speech and yet security, how you can have privacy yet security and lawyers, newspaper people, people in industry have been walking that fine line for a long time.

What it requires is people in this instance who understand the technology, who also understand the legal issues and the constitutional principles applicable to this area. And that is why it is such a challenge to identify people who have the expertise, both in the law and in the technology that can give meaning to it for all of us. But you have -- that is the great balancing act of our democracy.

JIM: Do you think we can have both?

ATTORNEY GENERAL RENO: Yes.

MR. MILLER: On behalf of ITA, I concur. In fact, I hate to disagree with such a titan of industry as Mr. Dell, but I think without cyber security, you can't have privacy.

We had an incident a few months ago where a major online vendor who sold CDs online protected the privacy in the sense that they did not sell lists of their customers. They didn't give away information for marketing. They did all the right things in terms of the FTC privacy policy. Then someone stole their list by hacking in. So the privacy was all gone. Three hundred and some thousand credit cards were given away.

So they had the right privacy policy under the way the FTC defines it and the way the industry defines it, but everyone's privacy was lost because someone broke through the security. So I don't see that it's mutually exclusive. In fact, I think they're mutually supportive. Gentleman in the back had a question.

QUESTION: Yes, the Attorney General mentioned using some models from the non online world as mechanisms to demonstrate how they work together. I'd be interested in some of those cooperative models that she sees that are working today in the government in the non online world for law enforcement industries. Are there examples you can draw from?

ATTORNEY GENERAL RENO: I think you can draw a number of examples. When prosecutors and the banking industry work together, they can understand what can be effective, what can't, how they limit how they protect confidentiality. The bank understands that if the case is prosecuted, that there will be -- we can assure confidentiality. But I think much has been done in that area. Much has been done in the area of white collar crime.

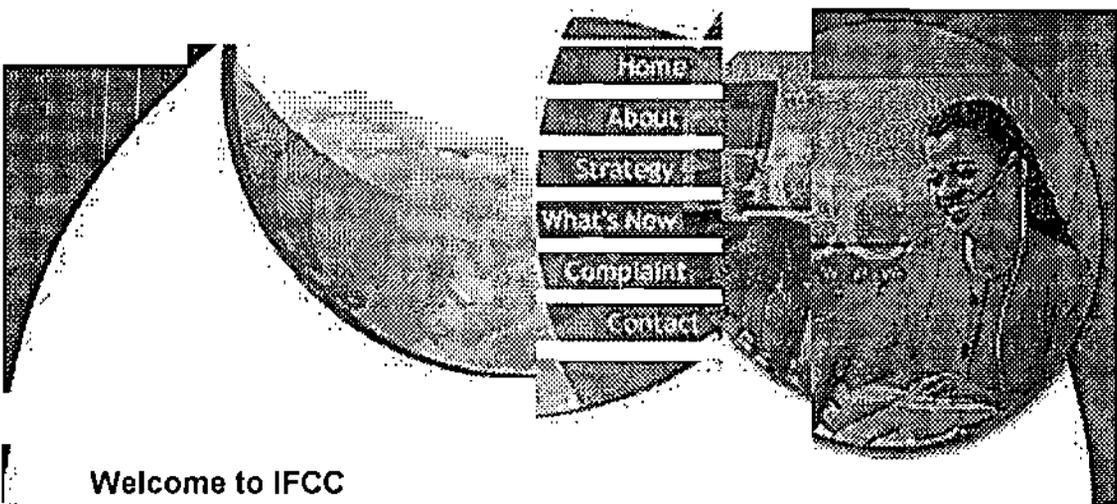
We have given much more attention in these last seven years to the whole issue of victims right in any area, whether it be terrorism, violent crime, white collar crime and similar instances.

And what it comes down to -- and I was going to make sure that I heard from everyone before I made this announcement. I'm asking the U.S. attorneys in the 93 districts across the country to sit down with industry in their communities to make sure that they establish the contacts.

There is nothing so effective as an FBI agent who knows what she or he is doing in the cyber world who goes to the banker and says let's sit down and talk. Or goes to the bank's security officer and says let's sit down and talk and then goes back and gets the SAC from the FBI to go talk to the bank president about security. And it really can make a difference. But it really comes down to personal contact.

So in terms of nationwide, I would hesitate to tell you that everything is perfect nationwide. I can tell you that where industry and the investigators come together and the prosecutors come together there is tremendous cooperation, understanding and I think successful prosecutions are resulting.

MR. MILLER: General Reno, thank you very, very much for taking your time. We look forward to seeing you this afternoon. Dick Brown, again, thank you for hosting this and for being with us today. We'll now have a 20 minute coffee break. Please be back in your seats at 10:30 when we'll have a chance for everyone to introduce himself or herself and also review what came out of the meeting that was held in Silicon Valley in April. Thank you, very much. Please thank the Attorney General and Dick Brown.



Welcome to IFCC

Welcome to the Internet Fraud Complaint Center. The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).



Data | Tools | Resources
File Now



IFCC's mission is to address fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation. For law enforcement and regulatory agencies at all levels, IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

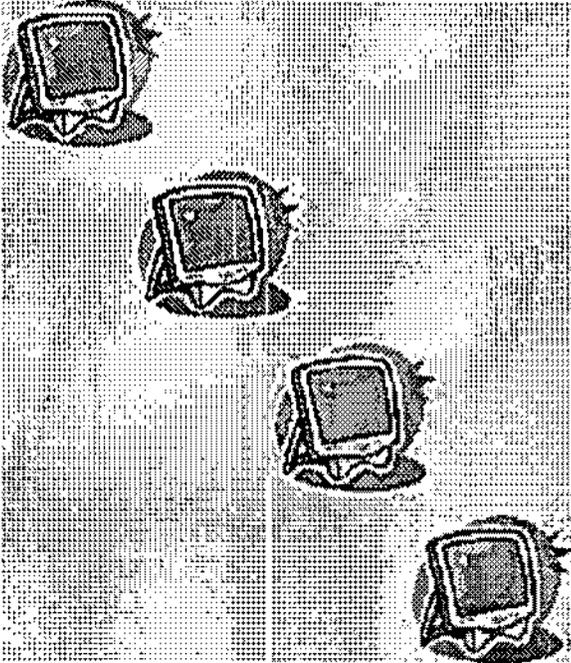
To visit the IFCC site map, [click here](#).

This program is brought to you by the [Federal Bureau of Investigation](#) and the [National White Collar Crime Center](#).

[top](#) | [home](#) | [about](#) | [strategy](#) | [what's new](#)
[complaint](#) | [contact](#) | [privacy](#) | [disclaimer](#) | [statistics](#)

©Copyright 2000 National White Collar Crime Center
All Rights Reserved

Text Only Version



Internet Fraud

- What Is Internet Fraud?
- What Are The Major Types of Internet Fraud?
- What Is The Department of Justice Doing About Internet Fraud?
- How Should I Deal With Internet Fraud?
- How Can I Get More Information About Internet Fraud?



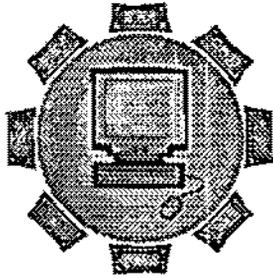
What Is Internet Fraud?

The term "Internet fraud" refers generally to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme.

If you use the Internet with any frequency, you'll soon see that people and things online tend to move, as the saying goes, on "Internet time." For most people, that phrase simply means that things seem to happen more quickly on the Internet -- business decisions, information-searching, personal interactions, to name a few - and to happen before, during, or after ordinary "bricks-and-mortar" business hours.

Unfortunately, people who engage in fraud often operate in "Internet time" as well. They seek to take advantage of the Internet's unique capabilities -- for example, by sending e-mail messages worldwide in seconds, or posting Web site information that is readily accessible from anywhere in the world - to carry out various types of fraudulent schemes more quickly than was possible with many fraud schemes in the past.

[DOJ Home Page](#) | [Fraud Section Home Page](#) | [Back to Top](#)



What Are the Major Types of Internet Fraud?

In general, the same types of fraud schemes that have victimized consumers and investors for many years before the creation of the Internet are now appearing online (sometimes with particular refinements that are unique to Internet technology). With the explosive growth of the Internet, and e-commerce in particular, online criminals try to present fraudulent schemes in ways that look, as much as possible, like the goods and services that the vast majority of legitimate e-commerce merchants offer. In the process, they not only cause harm to consumers and investors, but also undermine consumer confidence in legitimate e-commerce and the Internet.

Here are some of the major types of Internet fraud that law enforcement and regulatory authorities and consumer organizations are seeing:

- **Auction and Retail Schemes Online.** According to the Federal Trade Commission and Internet Fraud Watch, fraudulent schemes appearing on online auction sites are the most frequently reported form of Internet fraud. These schemes, and similar schemes for online retail goods, typically purport to offer high-value items - ranging from Cartier® watches to computers to collectibles such as Beanie Babies® - that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods).
- **Business Opportunity/"Work-at-Home" Schemes Online.** Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from \$35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.
- **Identity Theft and Fraud.** Some Internet fraud schemes also involve identity theft - the wrongful obtaining and using of someone else's personal data in some way that involves fraud or deception, typically for economic gain.
 - In one federal prosecution, the defendants allegedly obtained the names and Social Security numbers of U.S. military officers from a Web site, then used more than 100 of those names and numbers to apply via the Internet for credit cards with a Delaware bank.

- In another federal prosecution, the defendant allegedly obtained personal data from a federal agency's Web site, then used the personal data to submit 14 car loan applications online to a Florida bank.

- **Investment Schemes Online**

- **Market Manipulation Schemes.** Enforcement actions by the Securities and Exchange Commission and criminal prosecutions indicate that criminals are using two basic methods for trying to manipulate securities markets for their personal profit. First, in so-called "pump-and-dump" schemes, they typically disseminate false and fraudulent information in an effort to cause dramatic price increases in thinly traded stocks or stocks of shell companies (the "pump"), then immediately sell off their holdings of those stocks (the "dump") to realize substantial profits before the stock price falls back to its usual low level. Any other buyers of the stock who are unaware of the falsity of the information become victims of the scheme once the price falls.
 - For example, in one federal prosecution in Los Angeles, the defendants allegedly purchased, directly and through another man, a total of 130,000 shares in a bankrupt company, NEI Webworld, Inc., whose assets had been liquidated several months earlier. The defendants then allegedly posted bogus e-mail messages on hundreds of Internet bulletin boards, falsely stating that NEI Webworld was going to be taken over by a wireless telecommunications company. At the time of the defendants' alleged purchases of NEI Webworld stock, the stock was priced between 9 cents and 13 cents a share. Ultimately, in a single morning of trading, NEI Webworld stock rose in 45 minutes from \$8 per share to a high of \$15 5/16, before falling, within a half-hour, to 25 cents per share. The defendants allegedly realized profits of \$362,625.
 - In another federal prosecution in Los Angeles, a man who worked for a California company, PairGain Technologies, created a bogus Bloomberg news Web site which falsely reported that PairGain was about to be acquired by an Israeli company, and posted fraudulent e-mail messages, containing links to the counterfeit Bloomberg news site, on financial news bulletin boards. On the day that the bogus report was posted on the Internet, PairGain stock rose approximately 30 percent before PairGain issued its own press release stating that the report was false.

Second, in short-selling or "scalping" schemes, the scheme takes a similar approach, by disseminating false or fraudulent information in an effort to cause price decreases in a particular company's stock.

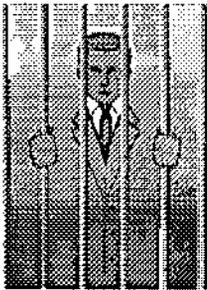
- For example, in one recent federal prosecution, a man who described himself as a "day trader" allegedly posted (more than 20 times) a bogus press release

falsely stating that a major telecommunications- and Internet-related company, Lucent Technologies, Inc., would not meet its quarterly earnings estimates. The day trader allegedly traded approximately 6,000 shares of Lucent stock the same day that he posted the bogus press release. The false reports allegedly drove the stock's price down 3.6 percent and reduced Lucent's market value by more than \$7 billion.

- **Other Investment Schemes** Other types of fraudulent investment schemes may combine uses of the Internet with traditional mass-marketing technology such as telemarketing to reach large numbers of potential victims.
 - In a federal prosecution in San Diego, a major fraudulent scheme used the Internet and telemarketing to solicit prospective investors for so-called "general partnerships" involving purported "high-tech" investments, such as an Internet shopping mall and Internet access providers. The scheme allegedly defrauded more than 3,000 victims nationwide of nearly \$50 million.
 - **Credit-Card Schemes.** Some Internet fraud schemes, which appear to be variations on the online auction schemes described earlier, involve the use of unlawfully obtained credit card numbers to order goods or services online.
 - One widely reported and intricate scheme, for example, involves offering consumers high-value consumer items, such as video cameras, at a very attractive price (i.e., below the price set at legitimate e-commerce Web sites). When a potential consumer contacts the "seller," the "seller" promises to ship the consumer the item before the consumer has to pay anything. If the consumer agrees, the "seller" (without the consumer's knowledge) uses that consumer's real name, along with an unlawfully obtained credit card number belonging to another person, to buy the item at a legitimate Web site. Once that Web site ships the item to the consumer, the consumer, believing that the transaction is legitimate, then authorizes his credit card to be billed in favor of the "seller" or sends payment directly to the "seller."
- As a result, there are two victims of the scheme: the original e-commerce merchant who shipped the item based on the unlawfully used credit card; and the consumer who sent his money after receiving the item that the "seller" fraudulently ordered from the merchant. In the meantime, the "seller" may have transferred his fraudulent proceeds to bank accounts beyond the effective reach of either the merchant or the consumer.
- **Other Schemes.** Some Web sites on the Internet have purported to offer those who want a "quick divorce" an opportunity to obtain a divorce in the Dominican Republic or other foreign countries for \$1,000 or more, without even having to leave the United

States. These sites often contain false, misleading, or legally inaccurate information about the process for obtaining such divorces (e.g., that neither spouse has to visit the country in which the divorce is being sought). Typically, people who have sent money to one of these schemes eventually receive false assurances that they are legally divorced. In fact, victims of the scheme have neither received legitimate legal services nor obtained valid divorces. People who are interested in obtaining a divorce, whether in the United States or elsewhere, should seek a lawyer with whom they can speak personally, and not rely solely on e-mail exchanges or online information.

[DOJ Home Page](#) | [Fraud Section Home Page](#) | [Back to Top](#)



What Is The Department of Justice Doing About Internet Fraud?

Since February 1999, when the Department of Justice established its Internet Fraud Initiative, the federal government has been expanding its efforts to combine criminal prosecution with coordinated analysis and investigation as part of a comprehensive approach to combating Internet fraud.

Prosecution

The Justice Department has begun to bring a number of criminal prosecutions throughout the country against individuals and groups engaging in various types of Internet fraud. Here are some examples of federal criminal prosecutions directed at Internet fraud:

- **Auction and Retail Schemes Online**

- *Oxford, Mississippi* On August 27, 1998, a woman was sentenced in the Northern District of Mississippi to 15 months' imprisonment and \$9,432 restitution on fraud charges relating to her conduct of a fraudulent scheme. The scheme involved her use of Web pages and interactive computer locations on the Internet for falsely advertising various computer hardware and software and computer accessories.
- *Philadelphia* On March 2, 2000, three men were criminally charged in the Eastern District of Pennsylvania for their alleged roles in falsely offering the sale of Beanie

Babies® on the Internet, and then failing to deliver the orders or sending stolen Beanie Babies® that generally were of substantially less value than the items ordered.

- *San Diego* On March 6, 2000, a man pleaded guilty in the Southern District of California to mail and wire fraud in connection with his conduct of a fraudulent scheme involving Internet sales of Beanie Babies® that he never delivered.
- *Santa Ana, California* On November 1, 1999, a man was sentenced in the Central District of California on mail and credit-card fraud charges to 14 months' imprisonment and \$36,000 restitution, for his conduct of an Internet auction fraud that falsely offered digital cameras and laptop computers to consumers.
- *Seattle* On August 6, 1999, a man pleaded guilty in the Western District of Washington to wire fraud in connection with his role in placing on various Web sites false advertisements for computer systems, for which he accepted victims' payments but which he never delivered.
- *West Palm Beach, Florida* On February 12, 1999, a man was sentenced in the Southern District of Florida on wire fraud charges to six months home detention and more than \$22,000 restitution, for his conduct of a fraudulent scheme in which he falsely advertised on Internet auction and retail sale Web sites computer components that he purported to have for sale, but did not have or obtain most of the merchandise he advertised.

- **Business-Opportunity Schemes Online**

- *Los Angeles* In November, 1999, four individuals were criminally charged in the Central District of California for their roles in conducting a fraudulent scheme, in which they sent out approximately 50 million e-mails that falsely advertised work-at-home opportunities for people but provided few actual opportunities for people who paid the \$35 advance fee.

- **Investment Schemes Online** "Pump-and-dump" schemes, short-selling schemes, Ponzi schemes, and other fraudulent investment schemes have all been subjects of federal prosecution throughout the country.

- *Alexandria, Virginia* In September 1997, a man was sentenced in the Eastern District of Virginia to one year's imprisonment and fined \$20,000 on securities fraud conspiracy charges relating to his touting of a stock involved in a "pump and dump" scheme.
- *Brooklyn, New York* In August, 1999, four individuals were indicted in the Eastern District of New York on securities fraud charges for their alleged roles in the fraudulent promotion of eight stocks through misleading Internet Web site and

e-mail newsletter profiles.

- *Charlotte, North Carolina* In 1999, two individuals pleaded guilty in the Western District of North Carolina to securities fraud charges for their roles in offering securities in a nonexistent investment bank that purportedly offered, among other things, a "guaranteed" 20 percent return on savings.
- *Cleveland* On March 22, 2000, four people were indicted in the Northern District of Ohio, on charges including conspiracy to commit and committing mail and wire fraud. The defendants allegedly devised and carried out a scheme to defraud "investors" in a "Ponzi" pyramid scheme. A company with which the defendants were affiliated allegedly collected more than \$26 million from "investors" without selling any product or service, and paid older investors with the proceeds of the money collected from the newer investors.
- *Los Angeles* On January 4, 2000, two men were indicted in the Central District of California on securities fraud charges for their alleged roles in the NEI Webworld scheme described earlier. In addition, on August 30, 1999, the individual who conducted the PairGain Technologies scheme mentioned earlier was sentenced in the Central District of California to five months' home detention and \$93,000 restitution.
- *New York* On August 9, 1999, a man was criminally charged in the Southern District of New York with securities fraud. The man allegedly conducted a scheme to unlawfully inflate the price of stock of a company involved in acquiring retail auto dealerships, by making various false claims that another company (located in the same office suite as the auto dealership company) had developed a cure for HIV infection and AIDS.

• Credit Card Fraud

- *Ft. Lauderdale* In November, 1997, a former graduate student was sentenced in the Southern District of Florida on wire fraud charges to four months' home detention, for a scheme in which he obtained the names of multiple students from a local university and fraudulently applied for 174 credit cards via the Internet. Because of the quick investigative work by the Postal Inspection Service, no losses were incurred.
- *Wilmington, Delaware* In 2000, three individuals were indicted in the District of Delaware on charges of conspiracy, bank fraud, identity theft, Social Security fraud, and wire fraud, for their alleged roles in the military officers' Social Security number/credit-card fraud scheme described earlier.

• Other Types of Internet Fraud

- *Los Angeles* On February 7, 2000, a man was sentenced to 87 months' imprisonment for his role in a scheme that purported to provide immigration assistance to aliens seeking to become residents or citizens of the United States. Using Web sites, newspaper advertisements, recruiters, and word of mouth to offer their services to aliens, the leaders of the scheme typically charged more than \$10,000 per client and promised that the client would receive particular immigration documents. In some cases, however, the leaders of the scheme provided their clients with counterfeit or false immigration documents; in other cases, they provided no documents at all, and blamed the government and the legal system for the delay in providing the promised documents.
- *Los Angeles* In November, 1999, four men were criminally charged in the Central District of California for their alleged roles in conducting the "work-at-home" scheme described earlier.

National Coordination and Cooperation

The global nature of the Internet, and law enforcement experience in conducting Internet fraud investigations, have made it increasingly clear that law enforcement authorities need to work in closer coordination to have a substantial effect on all forms of Internet fraud. Two major steps that the Department has taken to foster national coordination and cooperation among law enforcement authorities on Internet fraud matters are the Internet Fraud Initiative and the Internet Fraud Complaint Center.

- Internet Fraud Initiative The Internet Fraud Initiative, which the Attorney General approved on February 26, 1999, is a national initiative by the Department of Justice intended to provide a comprehensive approach to combating Internet fraud. The Initiative has six main elements:
 - (1) Developing information on the nature and scope of the problem, through coordination with the Federal Trade Commission on Internet fraud data, and exploring the development of methods for reliable estimates of the prevalence and incidence of Internet fraud;
 - (2) Developing and providing specific joint training for prosecutors and agents on Internet fraud, through National Advocacy Center (NAC) training at basic and advanced levels, other federal law enforcement training programs, and coordination with joint training efforts by the National Association of Attorneys General and the American Prosecutors Research Institute for state and local law enforcement;
 - (3) Fostering the development of investigative and analytical resources to identify and investigate Internet-related fraud schemes, by supporting joint FBI-National White Collar Crime Center efforts to establish the Internet Fraud Complaint Center and forging closer ties and establishing referral procedures with other federal

agencies;

(4) Providing and facilitating coordination among federal prosecutors, the Department and other federal law enforcement and regulatory agencies, and state, local, and foreign law enforcement agencies on Internet fraud investigations and prosecutions;

(5) Supporting and advising on Internet fraud prosecutions throughout the country; and

(6) Establishing a program of public education and prevention on Internet fraud, including encouraging the private sector to use technological solutions (such as biometrics) to prevent frauds, adding Internet fraud pages to the Department's Web site, and expanding public-private prevention efforts;

- Internet Fraud Complaint Center The Internet Fraud Complaint Center (IFCC) is a joint project of the FBI and the National White Collar Crime Center. The IFCC's key functions for federal, state, and local law enforcement agencies will be (1) receiving online complaints, (2) analyzing them to identify particular schemes and general crime trends in Internet fraud, and (3) compiling and referring potential Internet fraud schemes to law enforcement. In addition to FBI and NWCCC personnel, the IFCC will include agents and analysts detailed from the Internal Revenue Service and Postal Inspection Service.

In effect, the IFCC provides federal, state, and local law enforcement agencies with a single point of contact - a "one-stop-shopping" approach - for identifying and referring Internet fraud schemes for criminal enforcement. Because criminal fraud schemes on the Internet, such as major investment or credit card frauds, can be initiated and concluded in a matter of days or even hours, traditional methods of investigating fraud schemes will no longer suffice. By co-locating agents and analysts from the FBI, the NWCCC, and other agencies, the IFCC can provide a substantial investigative and analytical resource available on a nationwide basis to law enforcement and regulatory agencies.



How Should I Deal With Internet Fraud?

Judging by the sheer number of solicitations and "can't miss" propositions that you can see every day in your e-mail mailbox or posted on message boards or Web sites, Internet scams may seem inescapable. While you can't wholly avoid seeing online solicitations that may be fraudulent, here are some tips on how to deal with them.

GENERAL TIPS ON POSSIBLE INTERNET FRAUD SCHEMES

- **Don't Judge by Initial Appearances.** It may seem obvious, but consumers need to remember that just because something appears on the Internet - no matter how impressive or professional the Web site looks - doesn't mean it's true. The ready availability of software that allows anyone, at minimal cost, to set up a professional-looking Web site means that criminals can make their Web sites look as impressive as those of legitimate e-commerce merchants.
- **Be Careful About Giving Out Valuable Personal Data Online.** If you see e-mail messages from someone you don't know that ask you for personal data - such as your Social Security number, credit-card number, or password - don't just send the data without knowing more about who's asking. Criminals have been known to send messages in which they pretend to be (for example) a systems administrator or Internet service provider representative in order to persuade people online that they should disclose valuable personal data. While secure transactions with known e-commerce sites are fairly safe, especially if you use a credit card, nonsecure messages to unknown recipients are not.
- **Be Especially Careful About Online Communications With Someone Who Conceals His True Identity.** If someone sends you an e-mail in which he refuses to disclose his full identity, or uses an e-mail header that has no useful identifying data (e.g., "W6T7S8@provider.com"), that may be an indication that the person doesn't want to leave any information that could allow you to contact them later if you have a dispute over undelivered goods for which you paid. As a result, you should be highly wary about relying on advice that such people give you if they are trying to persuade you to entrust your money to them.
- **Watch Out for "Advance-Fee" Demands.** In general, you need to look carefully at any online seller of goods or services who wants you to send checks or money orders immediately to a post office box, before you receive the goods or services you've been promised. Legitimate startup "dot.com" companies, of course, may not have the

brand-name recognition of long-established companies, and still be fully capable of delivering what you need at a fair price. Even so, using the Internet to research online companies that aren't known to you is a reasonable step to take before you decide to entrust a significant amount of money to such companies.

TIPS ON SPECIFIC INTERNET FRAUD SCHEMES

- AUCTION AND RETAIL SALES SCHEMES

To reduce the chances that you may be victimized by fraudulent online auction or retail sales schemes, here are two basic tips:

- **Research The Prospective Seller Carefully.** If you haven't had personal (and favorable) experience with someone who's offering certain goods for online sale or auction, look for sources of information at the Web site where the offeror's information is posted, and at other Web sites. Some online auction sites provide their member with opportunities to provide "feedback" on their experiences with particular sellers (although certain sellers have tried to manipulate the "feedback" process by posting favorable but false reports about themselves).
- **Pay by Credit Card or Escrow Service If Possible.** If you charge your online purchase on a major U.S. bank-issued credit card, your liability may be limited to \$50 under any circumstances, and at least one credit-card issuer has recently indicated that it will waive the \$50 deductible. In the alternative, some online auction Web sites offer escrow services that (for a small percentage) will guarantee delivery of the ordered goods before releasing your payment to the seller.

- INVESTMENT SCHEMES ONLINE

To reduce your risks from online investment opportunities that may be fraudulent, here are four basic tips:

- **Take Your Time In Making Investment Decisions.** Remember that in any "get-rich-quick" scheme, there's only one person who's guaranteed to get rich quick: the person promoting the scheme.
 - If you're thinking about pursuing some online investment opportunity, start by recognizing that you need to take your time in making decisions about what you do with your hard-earned money. Sound investing for the long term takes patience, the will to ignore momentary market fluctuations, and a carefully thought-out plan for reaching your investment goals.
 - Whether you're researching an investment opportunity on the Web, or talking with a broker or someone else who's offering you the opportunity, you should make it a

habit to take notes of what you're reading or hearing. The North American Securities Administrators Association (NASAA) publishes an investor's notepad entitled, "When Your Broker Calls, Take Notes!" The forms are printed in notepad fashion so investors can get into the habit of making written records of their conversations with their brokers. The notepad is available from your state securities regulators or on the NASAA website at www.nasaa.org/whoweare/imedia/Notepad.html.

- **Research The Potential Investment Opportunity - And Who's Behind It - Carefully.** If you're making a major investment decision, here's an easy rule of thumb: Count how many weeks, months, or years it took you to earn that amount of money, and then resolve to spend at least that many days to research the investment opportunity and the people who are promoting or running it.
 - Several agencies and self-regulatory organizations can give you a substantial hand with your research, at no cost to you:
 - The SEC's Web site, www.sec.gov, contains a wealth of information about many companies, in at least two principal sources: (1) reports these companies file electronically through the EDGAR system; and (2) the SEC Enforcement Division's online files, which among other things list the persons against whom the SEC has filed civil enforcement actions for securities law violations (and, in some cases, against whom the Department of Justice or state or local prosecutors have filed criminal charges). You can use the built-in search engine at the SEC's Web site to check out names, and see whether you get any hits in the SEC enforcement action listings. The site also contains some excellent lists of questions to ask about any investment opportunity, and a discussion of how to spot signs of online investment scams.
 - The Federal Trade Commission's Web site, www.ftc.gov, also has an internal search engine, which allows you to look for information on particular individuals or companies involved with your prospective investment, including listings of FTC enforcement actions.
 - The National Association of Securities Dealers (NASD) allows you to check for some disciplinary history on the broker or company that's touting a particular investment. Go to www.nasdr.com or call the NASD's Public Disclosure hotline at 800-289-9999.
 - State securities regulators in your state may also have information on the company or its organizers that you can obtain. Check your local telephone listings for the securities regulator in your state, or go to the North American Securities Administrators Association's Web site, www.nasaa.org, for a

listing of state and provincial securities regulators in the United States, Canada, and Mexico.

- If the potential investment involves commodities, you may also need to check out the Commodity Futures Trading Commission's Web site, www.cftc.gov, and use its internal search engine to check out companies and people. The National Futures Association can also give you information on the disciplinary history of brokers or other commodity professionals, the registration status of firms and individuals, and arbitration and mediation procedures. Call them at 1-800-676-4NFA between 8:00 a.m. and 5:00 p.m. Central Time or go to www.nfa.futures.org.
- If the prospective investment supposedly involves an Internet financial institution, go to the Federal Deposit Insurance Corporation (FDIC)'s Online Banks Web pages, www.fdic.gov/bank/individual/online/sspcious.html, and use the FDIC's Financial Institutions Search Engine you find there to see whether the financial institution has a legitimate banking charter and is a member of the FDIC.
- When the potential investment is based outside the United States, remember that your money may be even more at risk, as you may have little or no recourse in the event of loss. The United Kingdom's Financial Services Authority allows investors to check out U.K. and European Union-based investment offers at its Central Register (call 01-71-929-3652).
- Finally, use one or more of the many Internet search engines - like the ones available on your Web browser - to help you expand your research on the company's background and market performance.

If you use these resources, and find that one or more of the people behind your prospective investment has been subject to legal action, especially for investment offers, it's a very safe bet that the investment is a high risk at best and an outright scam at worst.

- **Boilers and "Boiler Rooms" Need High Pressure To Do Their Jobs.** If someone online is insisting that you invest right away, or telling you that someone else will get the "deal of a lifetime" if you wait, ask yourself at that moment whether you're feeling pressured and uncomfortable. If you are, that's a major red flag warning you away from the investment.
 - Legitimate businesspeople and brokers don't need to subject you to "high-pressure" tactics to make you commit to an investment decision before you're ready. That's why the operations scam artists run are called "boiler rooms": like steam boilers, high pressure is what they're designed to generate (along with a wide array of lies, half-truths, and deceptive statements).

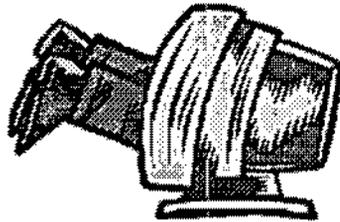
- Even if you're in a chat room or online discussion group where everyone seems to be "just like you," enthusiastic about investing and looking for the next great investment, not everyone who's online at that moment is necessarily just like you. Some of the messages you see may be coming from someone working for the investment scheme's organizers - or even one of the organizers himself - who pretends to be someone else, so they can pressure you in less obvious ways and get you to fall for the scheme.
- **Check Out The Competition.** If someone's promising you returns on investment that are far above what you see in the financial pages of your newspaper or at your local bank, ask yourself how they can possibly guarantee those fabulous returns.
 - Sometimes it's because, as in any good old-fashioned Ponzi scheme, they're paying older investors with money that newer investors gave them, and they're trying to string out the fraud to rope in as many investors as possible. Sometimes it's because they'll promise you anything, but give you nothing once you've entrusted your money to them.
 - If, after you've gone through all of the steps listed above, you still feel like the prospective investment is worth considering, talk to a broker, financial adviser, or banker with whom you've done business for a while, and ask whether his or her firm or financial institution can offer you a comparable type of investment with less risk.
 - The chances are that they'll say no, but they'll be willing to take time with you to walk through the information you have about the prospective investment and point out the risks you may be taking, as well as possible alternative investments that offer more realistic returns.
 - You lose nothing by consulting an investment professional about any major investment decision - and you stand to lose a lot if you don't.

FILING COMPLAINTS ABOUT INTERNET FRAUD

If you think that you've been the victim of a fraud scheme that involved the Internet, you can file a complaint online with the Internet Fraud Complaint Center, a joint project of the FBI and the National White Collar Crime Center. In addition, you can file complaints about specific types of fraud complaints with the following agencies:

- *Commodities Fraud:* Commodity Futures Trading Commission (CFTC)
- *Consumer Fraud:* Federal Trade Commission
- *Securities Fraud:* SEC Enforcement Division Complaint Center or your state securities

regulators.



How Can I Get More Information About Internet Fraud?

There's a better way to get information about Internet fraud than just diving blindly into the Internet. A number of government and private organizations have online information about various aspects of Internet fraud: what it is, how it can occur, and what you can do about it. To help you learn more, we've attached a list of Web sites that you might find interesting and informative on Internet fraud and related topics.

[Note: All Web sites to which these pages cross-link are included as a service for the reader. Cross-links to non-governmental sites do not constitute an endorsement or approval of their content, or of the organizations responsible for that content, by the Department of Justice.]

Government Web Sites

[Commodity Futures Trading Commission](#)

[Consumer.gov](#)

[Computer Crime and Intellectual Property Section, Criminal Division, U.S.](#)

[Department of Justice](#)

[Federal Bureau of Investigation](#)

[Federal Trade Commission](#)

[Internet Fraud Complaint Center](#)

[Securities and Exchange Commission](#)

[U.S. Customs Service](#)

[U.S. Postal Inspection Service](#)

[U.S. Secret Service](#)

[U.S. Sentencing Commission](#)

[Washington State Attorney General](#)

Nongovernmental Web Sites

[American Association of Retired Persons](#)

[Better Business Bureau](#)

[BBBOnline](#)

[Internet Fraud Council](#)

[Internet Fraud Watch](#)

[Internet ScamBusters](#)

[National Association of Attorneys General](#)

[National Association of Securities Dealers Regulation](#)

[National Consumers League](#)

[National Fraud Information Center](#)

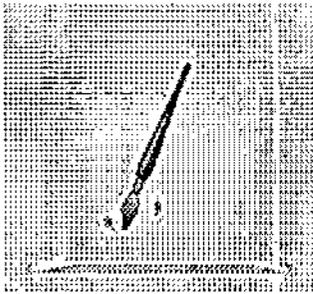
[North American Securities Administrators Association](#)

[SeniorNet](#)

[U.S. News & World Report Online - Citizen's Toolbox](#)

* * *

[DOJ Home Page](#) | [Fraud Section Home Page](#) | [Back to Top](#)



CREDITS

Design: Fraud Section, Criminal Division
U.S. Department of Justice, Washington, DC
Images: Corel

Last Updated: May 8, 2000
usdoj/criminal/fraud/jmh



Congressional Statement Federal Bureau of Investigation

March 16, 1999

Statement for the Record of
Michael A. Vatis
Director, National Infrastructure Protection Center
Federal Bureau of Investigation

on
**Critical Infrastructure Protection
and Information Warfare Issues**

Before the
Senate Armed Service Committee,
Subcommittee on Emerging Threats and Capabilities
Washington, D.C.

National Infrastructure Protection Center

INTRODUCTION

Mr. Chairman, Senator Bingaman, and Members of the Subcommittee: Thank you for inviting me here today to discuss critical infrastructure protection and information warfare issues. My brief remarks will focus on two areas: the role of the NIPC under Presidential Decision Directive-63 (PDD-63), and current impediments to critical infrastructure protection.

NIPC and PDD-63

PDD-63 creates an unprecedented set of intra-governmental as well as public-private cooperative structures for the vital mission of critical infrastructure protection. Let me begin by reviewing the roles assigned to the NIPC and the other key players in infrastructure protection.

PDD-63 authorized the expansion of the FBI's former organization, the Computer Investigations and Infrastructure Threat Assessment Center, into a full-scale National Infrastructure Protection Center. The PDD states that the NIPC "[s]hall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." It further states that the mission of the NIPC "will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response."

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

The NIPC has a vital role in collecting and disseminating information from all relevant sources. Thus, the PDD directs the NIPC to "sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in

appropriate form, to relevant federal, state, and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity." The NIPC is also charged with issuing "attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators."

In order to perform its role, the NIPC is establishing a network of relationships with a wide range of entities in both the government and the private sector. The PDD provides for this in several ways. First, it states that the Center will "include representatives from the FBI, US Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, Intelligence Community and Lead Agencies." Second, the NIPC will be "linked electronically to the rest of the government, including warning and operations centers as well as any private sector information sharing centers." Third, all executive departments and agencies are mandated to "cooperate with the NIPC and provide it assistance, information, and advice that the NIPC may request, to the extent permitted by law." Fourth, all executive departments are also mandated to "share with the NIPC information about threats and warning of attacks and actual attacks on critical government and private sector infrastructures, to the extent permitted by law." To ensure that the flow of information is unimpeded -- which is imperative when dealing with cyber attacks -- the PDD authorizes the NIPC to "establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create."

Let me address briefly why the NIPC is located at the FBI. First, as you know, the FBI has had existing programs and authorities to investigate computer crimes and to prevent and investigate acts of espionage and terrorism. These programs and authorities naturally support and mesh with the infrastructure protection mission. Second, in most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of his attack -- i.e., whether an intrusion is isolated or part of a broader pattern affecting numerous targets. This means it is often impossible to determine at the outset if an intrusion is an act of vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from the victim sites and intermediate sites such as Internet Service Providers and telecommunications carriers. Under our constitutional system, gathering such information usually requires some form of legal authority -- either criminal investigative or foreign counterintelligence. Thus, the NIPC is housed in the FBI to enable it to utilize the appropriate authorities to gather and retain the necessary information and to act on it. Now, this does not mean that the ultimate response to a cyber attack is limited to criminal investigation and prosecution. The response will be determined by the facts that are uncovered. Thus, for instance, if it is determined that a cyber intrusion is part of a strategic military attack, the President may determine that a military response is called for. But no such determination can be made without adequate factual foundation, and the NIPC's role is to coordinate the process for gathering the facts, analyzing them and making determinations about what is going on, and determining what responses are appropriate.

This role clearly requires the involvement and expertise of many agencies other than the FBI. This is why the NIPC, though housed at the FBI, is an interagency center that brings together personnel from all the relevant agencies. Thus, the Deputy Director is a civilian detailee from the Department of Defense; the Chief of our Analysis and Warning Section is a senior CIA analyst; and managers, investigators, analysts, and computer scientists within the Center come from across the defense, intelligence, and law enforcement communities. In addition, we are seeking infrastructure and technical experts from each of the infrastructure sectors to enhance our ability to understand and coordinate with the owners and operators of the infrastructures. Currently, the NIPC has representatives from multiple government agencies, including FBI, DOD, NSA, DOE, and CIA as well as federal and state law enforcement, including the U.S. Secret Service, the U.S. Postal Service, and, until recently, the Oregon State Police. Private sector representatives are also being sought. In fact, just yesterday the

Attorney General and the Information Technology Association of America announced a set of initiatives as part of a "Cybercitizens Partnership" between the government and the information technology (IT) industry. One initiative involves providing IT industry representatives to serve in the NIPC to enhance our technical expertise and our understanding of the information and communications infrastructure. This interagency, public-private composition will ensure that we are able to obtain information necessary to our mission from all relevant sources -- criminal investigations, intelligence sources, open sources, automated intrusion detection systems, and private sector contacts-- and that we are poised to coordinate closely with the other agencies that may need to participate in the response to an incident.

Other entities are also created by the PDD. The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism is responsible for overall policy implementation of the PDD. In this capacity he chairs the interagency Critical Infrastructure Coordinating Group. The PDD also created a National Planning Staff (renamed the Critical Infrastructure Assurance Office, or CIAO) to assist the National Coordinator in this policy function by coordinating the drafting of a "national plan" and the implementation of a national education and awareness program. The national plan is currently in the drafting process and is the subject of ongoing interagency discussions.

The PDD also designates certain agencies as the "lead agencies" for each infrastructure sector. These agencies (listed in footnote 1 on page 2) are charged with working with their respective Sectors (via a "Sector Coordinator" chosen to represent the sector) to: assess sector vulnerabilities and develop a plan to eliminate the significant ones; propose a system for identifying and preventing attempted major attacks; and develop a plan for alerting, containing and rebuffing an attack in progress and then reconstituting minimum essential capabilities in the aftermath of an attack. Given its roles in the areas of vulnerability, warning, response, and reconstitution monitoring, the NIPC needs to work closely with the Sector Coordinators and Liaisons in the development, implementation, and testing of their plans.

Finally, under the PDD the federal government is encouraging the creation of one or more Information Sharing and Analysis Centers (ISACs) by the private sector. As envisioned, the ISAC(s) "could serve as a mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC." ISACs could also serve to further disseminate NIPC information to industry. The provision of timely and complete information to the NIPC is critical for the success of its mission, and the PDD states that the ISACs are "not to interfere with direct information exchanges between companies and the government." As the government and private sector consider possible models for an ISAC, it is critical that nothing be created that would impede or delay the flow of incident and threat information to and from the NIPC. Rather, any ISAC should be designed to expedite the flow of information to enable real-time detection, analysis, and response by the NIPC.

Status of the NIPC and its Implementation of the PDD.

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

- The Computer Investigations and Operations Section (CIOS) is the operational and response arm of the Center. It program manages computer intrusion investigations conducted by FBI Field Offices throughout the country; provides subject matter experts, equipment, and technical support to cyber investigators in federal, state, and local government agencies involved in critical infrastructure protection; and provides a cyber emergency response capability to help resolve a cyber incident.
- The Analysis and Warning Section (AWS) serves as the indications and warning arm of the NIPC, provides analytical support during computer intrusion investigations, and performs long-term analyses of vulnerability and threat trends. When appropriate, it distributes tactical warnings and analyses to all the relevant partners, informing them of potential vulnerabilities and threats and

long-term trends. It also reviews numerous government and private sector databases, media, and other sources daily to gather information that may be relevant to any aspect of our mission, including the gathering of indications of a possible attack.

- The Training, Administration, and Outreach Section (TAOS) coordinates the training and education of cyber investigators within the FBI Field Offices and other federal, state and local law enforcement agencies. It also coordinates our outreach to private sector companies, state and local governments, other government agencies, and the FBI's field offices. In addition, this section manages our collection and cataloguing of information concerning "key assets" -- i.e., critical individual components within each infrastructure sector, such as specific power grids, telecommunications switch nodes, or financial systems -- across the country.

The NIPC is also developing its threat assessment, analytical, and warning capabilities. NIPC assessments form the basis for a variety of products, including alerts and advisories, an Infrastructure Protection Digest, a Y2K Report, a weekly update, CyberNotes, and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law through the NIPC Watch and Warning Unit. For example, the Infrastructure Protection Digest is a quarterly publication for sharing analysis and information on critical infrastructure issues. The Digest provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is published in a classified format and reaches national security and civilian government agency officials. Cybernotes is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published twice a month on our website and disseminated hardcopy to government and private sector audiences.

In addition, the NIPC is developing processes to ensure that we get relevant information in real time or near real time from all relevant sources, including: the US Intelligence Community, FBI criminal investigations, the private sector, other federal agencies, emerging intrusion detection systems, and open sources. This information is quickly analyzed to determine if a broad scale attack is underway. If we determine an attack is underway, we can issue warnings using an array of mechanisms, and send out sanitized and unsanitized warnings to the appropriate parties in Federal Government and the private sector so they can take immediate protective steps. This is a difficult process requiring the design of both procedures for reporting and sanitization, and collection and distribution mechanisms. The NIPC is currently working on these procedures and mechanisms. The long-term goal is to develop a comprehensive "indications and warning" system. This will require participation by the Intelligence Community, DOD, the sector lead agencies, other government agencies, federal, State and local law enforcement, and the private sector owners and operators of the infrastructure. Currently, the NIPC is focusing on developing and implementing a methodology and system for detecting and warning of attacks on the federal government and the national telecommunications and electric power sectors.

Response is central to the NIPC mission. To facilitate our ability to investigate and respond to attacks, the FBI has created a National Infrastructure Protection and Computer Intrusion Program in the 56 FBI field offices across the country. Under this program, managed by the NIPC at FBIHQ, full "NIPCI" squads or smaller teams have been created in each field office to conduct computer intrusion investigations, respond to threats, and collect information on "key assets" within each sector. There are currently 10 full NIPCI squads in Washington DC, New York, San Francisco, Chicago, Dallas, Los Angeles, Atlanta, Charlotte, Boston, and Seattle. The other field offices have smaller teams. The 10 squads have regional responsibilities, assisting the smaller teams in other offices when an incident exceeds the smaller team's resources or capabilities. Ultimately, we need to create a full squad in each field office. During the first nine months of 1998 the NIPCI squads and teams opened 377 new cases, closed 304 cases and had a pending caseload of 526 matters. Currently, there are 680 pending investigations of computer intrusion matters. The pending caseload is

expected to markedly increase in the coming years.

The program to protect and respond to physical attacks on the US critical infrastructure are handled by the FBI's counter-terrorism program. The NIPC supports this initiative through its management of the Key Asset Program (KAP). A key asset can be defined as an organization, group of organizations, system, or group of systems, or physical plant the loss of which would have widespread and dire economic or social impact on a national, regional, or local basis. The KAP initially will involve determining which assets are key within the jurisdiction of each FBI field office, obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if resources permit, the Program would include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets. FBI Field Offices will be responsible for developing a list of the assets within their respective jurisdictions, while the NIPC will maintain the national database. This program will be developed in coordination with DOD and other agencies. This program serves the critical needs of developing lists of the key assets within each critical infrastructure and also of developing the communications and liaison links necessary for the collection of information and the dissemination of warnings to the infrastructure owners and operators.

The FBI, in conjunction with the private sector, has also developed an initiative called "InfraGard" to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats. The initiative encourages the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each Field Office. Chapter membership includes representatives from the FBI, private industry, other government agencies, State and local law enforcement, and the academic community. The initiative provides four basic services to its members: an intrusion alert network using encrypted e-mail; a secure website; local chapter activities; and a help desk for questions. The critical component of InfraGard is the ability of industry to provide information on intrusions to the NIPC and local FBI field office using secure communications in both a "sanitized" and detailed format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation; while the NIPC can analyze that information in conjunction with other law enforcement, intelligence, or industry information to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. InfraGard, which began as a pilot program in the Cleveland, Cincinnati, and Indianapolis field offices, will be expanded to 14 additional offices this month, and to the rest of the country later this year.

The NIPC also serves as the U.S. government lead agency for the Emergency Law Enforcement Services Sector. As Sector Liaison for law enforcement, the NIPC and a Sector Coordinator representing the law enforcement sector are formulating a plan to reduce vulnerabilities of state and local law enforcement to attack and developing methods and procedures to share information within the sector. The NIPC and the FBI Field Offices are also working with the State and local law enforcement agencies to raise awareness with regard to vulnerabilities in this sector.

The NIPC has also been very active in training. Training FBI and other agencies' investigators is critical if we hope to keep pace with the rapidly changing technology and be able to respond quickly and effectively to computer intrusions. The NIPC trained 170 FBI agents and 17 representatives from other law enforcement agencies in 1998. We currently plan to train over 1000 law enforcement personnel in 1999 at the federal, state, and local levels. Additional training initiatives include specialized courses in information security developed by the private sector. Together, these efforts will help place us at the cutting edge of law enforcement and national security in the 21st Century.

Policy and Statutory Impediments to Combating Threats to the Critical

Information infrastructure.

There are several policy and statutory impediments to our being able to fully address the threats to the critical information infrastructure.

Hiring sufficient personnel for the National Infrastructure Protection Center and for the nationwide National Infrastructure and Computer Intrusion Program continues to be a major concern. The prevention, detection, analysis, warning, and response missions assigned to the NIPC and FBI field offices all require a large number of skilled personnel. Currently, we believe there are far more intrusions occurring than we know about or can investigate. Additional personnel are therefore a vital need if we are to learn about, investigate, and respond to attacks on our infrastructures. As use of the Internet continues to increase dramatically, the number of intrusions will grow even more, and our capability must keep pace.

I should note that some of the shortfall could be met with detailees from other agencies. Congress has prohibited us, however, from reimbursing other agencies for detailees in FY 99, which has naturally made it somewhat more difficult for other agencies to devote scarce resources to our common mission at the NIPC.

There are a number of statutory issues related to protecting the infrastructure. Fortunately, a number of agencies are focused on identifying these concerns with an aim towards working with the Congress to consider legislative fixes. The NIPC is coordinating in this regard with, among others, the Computer Crime and Intellectual Property Section of the Department of Justice's Criminal Division, the CIAO and the Security Policy Board.

Examples of some of the issues the NIPC or other members of the infrastructure protection community are concerned with include:

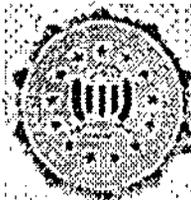
- the updating of federal trap and trace and pen register authorities in order to take account of new information technologies;
- the need for multi-jurisdictional pen register and trap and trace orders rather than multiple orders each covering one jurisdiction;
- the need to address sentencing issues regarding minors who commit computer crimes;
- the need to criminalize unauthorized computer access to sensitive computer and information networks when it is difficult to put a dollar value on the harm (since jurisdiction over many types of computer crimes currently attaches only at the \$5,000 mark);
- the need to create criminal forfeiture provisions for violations of the Computer Fraud and Abuse Act, so we can seize computers of convicted computer criminals;
- the need to clarify current law to unambiguously permit the United States to conduct domestic investigations and prosecutions when a United States computer is not itself the target of a computer crime but is used as a conduit to attack systems abroad.

CONCLUSION

PDD-63 established the NIPC as the operational linchpin of our efforts to protect America's critical infrastructures in the 21st century. Ours is a national mission to combine the inputs from the government lead agencies and the private sector in order to provide analyses and warnings and to respond to an intrusion incident. But the NIPC can perform this mission only if has the necessary resources, interagency support, and information from multiple sources. I believe we have made significant progress in the first year of our existence in establishing the foundation for an effective system for preventing, detecting, and responding to cyber attacks. In just this past year, we have brought on board over 100 personnel from many agencies at NIPC HQ; established a national program for computer investigations in every FBI

field office; developed and delivered advanced training in network investigations to nearly 200 FBI and other government agency investigators; developed several mechanisms and programs to share information with the private sector; begun a program to protect "key assets" with each infrastructure sector from cyber attack; and coordinated several national-level investigations involving numerous agencies and FBI field offices. While much has been accomplished, however, much work remains in developing our detection, prevention, warning, and response capabilities. I look forward to working with this Subcommittee and the Congress in protecting our national security against this difficult challenge.

Thank you.



Congressional Statement Federal Bureau of Investigation

July 26, 2000

Statement for the Record of
Michael A. Vatis, Director
National Infrastructure Protection Center
Federal Bureau of Investigation

on

The NIPC's International Response to Cyber Attacks and Computer Crime

Before the
House Committee on Government Affairs
Subcommittee on Government Management, Information, and Technology
Washington, D.C.

Good morning, Chairman Horn, Congressman Turner, members of the subcommittee, and distinguished guests. I am pleased to testify before this subcommittee today on our international response to cyber attacks and computer crime in general. The representation you have assembled for this hearing is truly extraordinary. To my knowledge, never have so many international law enforcement officials testified before Congress at one time on issues related to cyber intrusions and computer crime. A recently released study estimates that computer viruses and hacking take a toll of \$1.6 trillion on the global economy. This figure dwarfs the gross national product of most of the world's nations. Given the global nature of the computer crime problem and the fact that many of our investigations in the U.S. have an international nexus, it is vital that we work effectively across borders in concert with our international partners. I believe this hearing will contribute to that effort and highlight the extensive endeavors we have already made in the international arena.

Protecting the Nation's critical infrastructures and combating computer intrusions is by necessity a cooperative effort. National governments must work within themselves, across agencies; with regional and local law enforcement; with private industry; and with foreign governments to combat the problem. If cooperation is lacking in any one of these areas, the whole effort will fall short. Yet if cooperation is effective across all of these areas, then we can gain the upper hand against cyber criminals around the world and ensure that the Internet is a safe place for electronic commerce and communication.

Cooperative Structures in the United States

The U.S. government approach to protecting the nation's critical infrastructures is outlined in Presidential Decision Directive (PDD) 63, issued in May 1998. That Directive forms a series of cooperative arrangements. In particular, PDD-63 categorizes our infrastructures into several sectors and designates federal "Lead Agencies," which are responsible for working cooperatively with private industry from each sector to develop mechanisms and plans for securing that sector against cyber attacks and for recovering should an attack occur.

The PDD also gives a significant coordinating role for operational matters to the National Infrastructure Protection Center (NIPC), which I head. The PDD places the NIPC at the core of the government's warning, investigation, and response system for threats to, or attacks on, the nation's critical infrastructures. The NIPC is the focal point for gathering information on threats to the infrastructures as well as "facilitating and

coordinating the Federal Government's response to an incident." The PDD further specifies that the NIPC should include "elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach, and development and application of technical tools."

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

In order to perform its role, the NIPC has established, and is continuing to expand, a network of cooperative relationships with a wide range of entities in both the government and the private sector. First, the Center, while located at the FBI, is interagency in its composition, bringing together representatives from the law enforcement, defense, and intelligence communities, as well as from many of the lead agencies specified in the PDD. The Center currently has representatives from the following federal entities: Navy, Air Force, Army, Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, United States Postal Service, Federal Aviation Administration, General Services Administration, Central Intelligence Agency, Critical Infrastructure Assurance Office, and Sandia National Laboratory. In addition, the Center has had state law enforcement officials detailed on a rotating basis. So far we have had representatives from the Oregon State Police and the Tuscaloosa County (Alabama) Sheriff's Department. We also have international liaison officials who work with the Center. This interagency composition facilitates the NIPC's ability to share pertinent information among agencies and to coordinate agencies' activities in the event of an attack.

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

In addition, in its role under Presidential Decision Directive (PDD) 63 as the lead agency for the "Emergency Law Enforcement Sector" (ELES), the NIPC has been working with state and local law enforcement to develop a plan to protect that sector from cyber attack and reduce its vulnerabilities. As part of that effort, the NIPC's alerts and warnings are regularly sent to state and local law enforcement agencies via the National Law Enforcement Telecommunications System (NLETS) and through NIPC e-mail via the Law Enforcement Online system. Sharing with state and local law enforcement is critical because they are often the first responders when an incident occurs.

To fulfill its mandate under PDD-63, the NIPC's goal is to develop a comprehensive "indications and warning" system that will be capable of timely collection of indicators of an imminent or ongoing cyber attack, analysis of the information, and the timely issuance of alerts and warnings. This will require additional resources, both personnel and equipment. It will also require participation by the Intelligence Community; the Department of Defense; the sector "Lead Agencies"; other government agencies; federal, state and local law enforcement; and the private sector owners and operators of the infrastructures. As I will discuss further in a moment, the NIPC is currently working with industry to develop a methodology and system for detecting and warning of attacks on the national telecommunications and electric power sectors. These will

provide a model for possible systems for the other sectors.

Finally, the NIPC, as the national entity responsible for government's warning, investigation, and response system for threats to, or attacks on, the nation's critical infrastructures, works on national planning initiatives with the National Security Council and the Critical Infrastructure Assurance Office.

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

- The Computer Investigations and Operations Section (CIOS) is the operational and response arm of the Center. It program manages computer intrusion investigations conducted by FBI Field Offices and some of the joint task forces throughout the country; provides subject matter experts, equipment, and technical support to cyber investigators in federal, state, and local government agencies involved in critical infrastructure protection; and provides a cyber emergency response capability to help resolve a cyber incident.
- The Analysis and Warning Section (AWS) serves as the "indications and warning" arm of the NIPC. The AWS reviews numerous government and private sector databases, media, and other sources daily to collect and disseminate information that is relevant to any aspect of NIPC's mission, including the gathering of indications of a possible attack. It provides analytical support during computer intrusion investigations, performs analyses of infrastructure risks and threat trends, and produces current analytic products for the national security and law enforcement communities, the owners-operators of the critical infrastructures, and the computer network managers who protect their systems. It also distributes tactical warnings, alerts, and advisories to all the relevant partners, informing them of exploited vulnerabilities and threats.
- The Training, Outreach and Strategy Section (TOSS) coordinates the training and continuing education of cyber investigators within the FBI Field Offices and other federal, state and local law enforcement agencies. It also coordinates our liaison with private sector companies, state and local governments, other government agencies, and the FBI's Field Offices. In addition, this section manages our collection and cataloguing of information concerning "key assets" – i.e., critical individual components within each infrastructure sector, such as specific power facilities, telecommunications switch nodes, or financial systems – across the country.

To facilitate our ability to investigate and respond to attacks, the FBI has created the National Infrastructure Protection and Computer Intrusion (NIPCI) Program in the 56 FBI Field Offices across the country. We currently have 193 agents nationwide dedicated to investigating computer intrusion, denial of service, and virus cases (less than 2% of all FBI agents nationwide). In order to leverage these resources most efficiently, we have taken the approach of creating 16 regional squads that have sufficient size to work complex intrusion cases and to assist those field offices without a full NIPCI squad. In those field offices without squads, the FBI has established a baseline capability by having at least one or two agents to work NIPCI matters, i.e. computer intrusions (criminal and national security), viruses, the InfraGard and Key Asset Initiatives, and state and local liaison.

In addressing cyber incidents, the NIPC and the 56 FBI field offices work cooperatively with their federal, state and local law enforcement partners and with the private sector. For example, in the Melissa Macro Virus investigation, the NIPC issued public warnings that helped alert the public, government agencies, and private industry to the virus and stem the damage to computer networks. In addition, the FBI's Newark office worked closely with the New Jersey State Police, the New Jersey Attorney General's Office, and the U.S. Attorney's Office in New Jersey in the investigation, arrest, and prosecution of David L. Smith. The NIPC supported the overall investigation which spanned the nation. In other cases where there is concurrent jurisdiction, the FBI and other agencies often work cases jointly. For example, the FBI and the U.S. Secret Service worked together on a series of hacks into the White House Homepage. Eric

Burns, a.k.a Zyklon, hacked into the White House web site as well as other sites. He was caught and pled guilty to one count of 18 U.S.C.1030. In November 1999 he was sentenced to 15 months in prison, 3 years supervised release, and ordered to pay \$36,240 in restitution and a \$100 fine. While I cannot discuss it in open hearings, the NIPC also works closely with other agencies in foreign counter intelligence investigations involving cyber attacks.

Government-Industry Cooperation

As I noted earlier, however, it is critical for the government not just to work cooperatively within itself, but also with the private sector. The NIPC is engaged in several initiatives to work cooperatively with the private sector, principally in the area of information sharing. First, the NIPC, in conjunction with the private sector, has developed an initiative call "InfraGard" to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. The initiative encourages and facilitates the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each FBI Field Office. Chapter membership includes representatives from the FBI, private industry, other government agencies, state and local law enforcement, and the academic community. The critical component of InfraGard is the ability of industry to provide information on intrusions to the NIPC and to the local FBI Field Office, using secure communications, in both a "sanitized" and detailed format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation; the NIPC, in turn, can analyze that information in conjunction with other law enforcement, intelligence, and industry information to determine if the intrusion is part of a broader attack on numerous sites. The Center can simultaneously use the sanitized version to inform other members of the threat and the techniques used, without compromising the confidentiality of the reporting company. The secure website also contains a variety of analytic and warning products that we make available to the InfraGard community.

We believe InfraGard, once fully implemented, will be a significant step forward in enhancing the ability of the private sector and the government to share information with each other. The government has access to unique sources of information through its intelligence and law enforcement activities. These need to be shared, in appropriately sanitized form, with private sector owners and operators so that they can protect themselves against threats that we become aware of. Conversely, the private sector is often the victim of cyber attacks and threats that are highly relevant to our mission to protect that nation's critical infrastructures from attack. Only by bringing these governmental and private sources of information together can we get a sense of the full picture of threats and incidents, draw linkages, and engage in effective "indications and warning" regarding cyber attacks. In contrast to efforts to share information solely within one industry sector, InfraGard provides a vehicle for sharing information across sectors and between the government and industry generally.

A second effort involving cooperation with the private sector is the Key Asset Initiative (KAI). A key asset can be defined as an organization, system, group of organizations or systems, or physical plant, the loss of which would have widespread and dire economic or social impact on a national, regional, or local basis. The KAI initially involves determining which assets are "key" within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in case of an emergency. Eventually, contingent on future funding, the KAI will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets. FBI Field Offices are responsible for developing a list of the assets within their respective jurisdictions, while the Center maintains a national database. This initiative serves the critical needs of developing lists of the key assets within each critical infrastructure and also of developing the communications and liaison links necessary for the collection of information and the dissemination of warnings to the infrastructure owners and operators.

Another initiative is a pilot program we have developed with the North American Electrical Reliability Council (NERC) to develop an "Indications and Warning" System for physical and cyber attacks. Under the pilot program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. We see this initiative as a good example of government and industry working together to share information and it is our expectation that the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. We are currently working with industry on developing an Indications and Warning program for the telecommunications sector.

The NIPC has also been working on a set of outreach conferences under the auspices of the Department of Justice and the Information Technology Association of America. In April, 2000 the Attorney General, representatives from the NIPC, Special Agents from FBI Field Offices, and other law enforcement officials met with west coast industry representatives at Stanford University. Last month, we met with east coast industry representatives at EDS in Herndon, Virginia. At both conferences the Attorney General stressed ways that industry and law enforcement need to work together against computer hackers and intrusions. It was clear at both conferences, too, that industry wants a good, cooperative relationship with law enforcement to share information about threats and incidents, and to investigate cyber attacks successfully. A number of initiatives stemming from those conferences are currently underway to further this cooperative relationship.

NIPC representatives spend a significant portion of our time speaking across the country and around the world to private sector and government groups, as part of our effort to raise awareness about the cyber threat and to foster cooperation between industry and law enforcement. For example, we have recently participated in meetings of the National Security Telecommunications Advisory Committee (NSTAC), a private sector advisory committee to the President whose purpose is to provide advice and expertise on national security and emergency preparedness telecommunications policy); the System Administration, Networking, and Security (SANS) Institute, a cooperative research and education organization founded in 1989 for the purpose of sharing information among system administrators, security professionals, and network administrators; the Information Security Forum, an association of organizations who share best practices and other solutions to information security problems; the National Governors Association; the American Society for Industrial Security (ASIS), a 32,000 member organization for professionals responsible for security; and the American Bar Association (ABA).

Finally, the NIPC is working with the Critical Infrastructure Assurance Office in the Department of Commerce on outreach initiatives. All of these efforts are critical to the goal of building a partnership between industry and the government for the purpose of securing our nation's critical infrastructures and reducing our vulnerability to cyber crime.

NIPC and International Cooperation

Most pertinent to this hearing is the issue of cooperation across national borders. A typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Even intrusions into U.S. systems by a perpetrator operating within the U.S. often require international investigative activity because the attack is routed through Internet Service Providers and computer networks located outside the United States. When evidence is located within the United States, we can subpoena records, conduct electronic surveillance, execute search warrants, seize evidence, and examine it. We can do none of those things ourselves overseas to solve a U.S. criminal case. Instead, we must depend on the local authorities to assist us. This means that

effective international cooperation is essential to our ability to investigate cyber crime.

International investigations pose special problems. First, while the situation has improved markedly in recent years, many countries lack substantive laws that specifically criminalize computer crimes. This means that those countries often lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist us when evidence might be located in those countries. Moreover, the quickly evolving technological aspects of these investigations can exceed the capabilities of local police forces in some countries. Finally, even when countries have the requisite laws and have developed the technical expertise necessary to conduct cyber investigations, successful investigation in this arena requires more expeditious response than has traditionally been the case in international matters, because electronic evidence is fleeting and, if not secured quickly, can be lost forever.

NIPC international Outreach

The NIPC is working with its international partners on several fronts to address the issues outlined above. The first area consists of outreach activities designed to raise awareness about the cyber threat, encourage countries to address the threat through substantive legislation, and provide advice on how to organize to deal with the threat most effectively. Almost weekly the NIPC hosts a foreign delegation to discuss topics ranging from current cases to the establishment of NIPC-like entities in other nations. Since the NIPC was founded, Japan, the United Kingdom, Canada, Germany, and Sweden have formed or are in the process of forming interagency entities like the NIPC. The NIPC has briefed visitors from the United Kingdom, Germany, France, Norway, Canada, Japan, Denmark, Sweden, Israel, and other nations over the past year. In addition, to promote understanding of the NIPC mission, an "open house" for embassy personnel was held in March 2000.

Abroad, the FBI's Legal Attaches (Legats) are often the first officials contacted by foreign law enforcement should an incident occur. We are providing training to our Legats on how to coordinate computer intrusion and infrastructure protection matters with us to make them more effective. In addition, NIPC personnel are in almost daily contact with Legats around the world to assist in coordinating requests for information.

NIPC International Training

In order to help make our foreign partners more capable to assist our international investigations and to address cyber crime within their own countries, the NIPC has also provided training to investigators from several nations. Much of this training takes place at the International Law Enforcement Academies in Budapest, Hungary and Bangkok, Thailand. In addition, a small number of select international investigators receive training in NIPC sponsored classes in the United States. The NIPC also holds workshops with other nations to share information on techniques and trends in cyber intrusions. For example, in September 1999 the NIPC sponsored an International Cyber Crime Conference in New Orleans to provide training to international law enforcement officers and forge links between foreign law enforcement officers and personnel representing: the NIPC, FBI field offices, FBI Legats, the U.S. Secret Service, the Naval Criminal Investigative Service, the Air Force Office of Special Investigations, and the U.S. Postal Inspection Service.

The G-8 High-Tech Crime Working Group

Another international initiative that the NIPC has been involved in is the G-8's High-Tech Crime Subgroup of the G-8 "Lyon Group." A representative of the NIPC serves as a member of the United States delegation to the Subgroup, which has been considering several issues concerning international cyber crime investigations, including the establishment of a 24/7 high-tech crime points of contact network, international training conferences, review of legal systems in G-8 countries, and the development of the G-8 principles on transborder access to stored computer data.

The 24/7 high-tech points of contact network was established in March 1998. Each of the G-8 countries identified a point of contact for law enforcement in each of their respective countries. These contacts are required to be available twenty-four hours a day, seven days a week, in order to respond to requests for assistance in important high-tech crime investigations in which electronic evidence may either be altered or destroyed.

With regard to training, the subgroup hosted an international computer crime training conference in November 1998, for law enforcement investigators of the G-8 countries. This conference addressed law enforcement issues relating to high-tech crime investigations and the technical issues involved in these specific types of investigations. In addition, the subgroup has compiled a collection of the substantive and procedural laws regarding computer crimes in each of the G-8 countries. Regarding the critical issue of transborder access to stored data, the subgroup has provided recommendations for principles of transborder access to stored computer data. In addition, the subgroup has written principles that provide a mechanism to secure the rapid preservation of stored data in computer systems. These recommendations will attempt to prevent instances where computer data of possible evidentiary value is altered or deleted while a formal request for assistance under a Mutual Legal Assistance Treaty (MLAT) is processed. Lastly, the G-8 subgroup has referred the task of developing common terms and common formats for forensic requests and developing international standards for the retrieval and processing of electronic evidence to the International Organization of Computer Evidence (IOCE), which has representation in most of the G-8 countries.

In May 2000, the NIPC attended a G-8 industry/law enforcement conference in Paris, France. This meeting, which included individuals representing industry and consumer groups, was structured to allow both industry and law enforcement officials to share ideas and concerns regarding the security of the Internet. Each participating country's contingent consisted of industry and government representatives, from a variety of agencies, and each country had one industry and one government representative make a presentation to the group about issues concerning their nation. Government officials were sensitized to the concerns of both industry and consumers, and industry and the public representatives were exposed to some of the challenges facing law enforcement and other government agencies in their struggle to provide a safe, secure environment for e-commerce. A subsequent meeting building on the success of the Paris forum is planned for October 2000.

The NIPC and International Investigations

Since the creation of the NIPC in February 1998, we have seen a significant increase in the number of investigations requiring international cooperation. The NIPC has provided an effective vehicle for coordinating these investigations. I will provide a few examples to demonstrate the issues raised by such investigations and how they have been addressed by the NIPC.

One example is the Solar Sunrise case, the code name for a multi-agency investigation of intrusions into more than 500 military, civilian government, and private sector computer systems in the United States during February and March 1998. These intrusions occurred just as the NIPC was being established. The intrusions took place during the build-up of United States military personnel in the Middle East in response to tensions with Iraq over United Nations weapons inspections. The intruders penetrated at least 200 unclassified U.S. military computer systems, including seven Air Force bases and four Navy installations, Department of Energy National Laboratories, NASA sites, and university sites. The timing of the intrusions, and the fact that some activity appeared to come from an ISP in the Middle East, led many U.S. military officials to suspect that this might be an instance of Iraqi information warfare. The NIPC coordinated an extensive interagency investigation involving FBI Field Offices, the Department of Defense, NASA, Defense Information Systems Agency, Air Force Office of Special Investigations, the Department of Justice, and the Intelligence Community.

Internationally the NIPC worked closely with the Israeli law enforcement authorities. Within several days, the investigation determined that two juveniles in Cloverdale, California, and individuals in Israel were the perpetrators. This case demonstrated the critical need for an interagency center to coordinate our investigative efforts to determine the source of such intrusions and the need for strong international cooperation. Israeli authorities are preparing to prosecute the chief defendant in their case in the summer of 2000.

More recent cases demonstrate how much international cooperation has improved in this area. In February 2000, the NIPC received reports that CNN, Yahoo, Amazon, Com, e-Bay, and other e-commerce sites had been subject to "Distributed Denial of Service" (DDOS) attacks. The NIPC had issued warnings in December 1999 about the possibility of such attacks, and even created and released a tool that victims could use to detect whether their system had been infiltrated by an attacker for use against other systems. When attacks did occur in February, companies cooperated with the NIPC and our National Infrastructure Protection and Computer Intrusion Squads in several FBI field offices (including Los Angeles and Atlanta) and provided critical logs and other information. Within days, the FBI and NIPC had traced some of the attacks to Canada, and subsequently worked with the Royal Canadian Mountain Police to identify the suspect. The Royal Canadian Mounted Police (RCMP) arrested a juvenile subject in April 2000, and charges are expected to be brought shortly for at least some of the attacks. The unprecedented speed and scope of this investigation was evidence of the great improvement made in our ability to conduct large scale, complex international investigations.

Another example involves the compromise between January and March 2000 of multiple e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom by a hacker known as "Curador." Curador broke into the sites and apparently stole as many as 28,000 credit card numbers, with losses estimated to be at least \$3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) Police Service in a search at the residence of "Curador," whose real name is Raphael Gray. Mr. Gray, age 18, was arrested in the UK along with a co-conspirator under the UK's Computer Misuse Act of 1990.

This case was predicated on the investigative work by the FBI, the Dyfed Powys Police Service in the United Kingdom, Internet security consultants, the RCMP, 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.

Most recently, companies and individuals around the world by the "Love Bug," a virus (or, technically, a "worm") that traveled as an attachment to an e-mail message and propagated itself extremely rapidly through the address books of Microsoft Outlook users. Investigative work by the FBI's New York Field Office, with assistance from the NIPC, traced the source of the virus to the Philippines within 24 hours. The FBI then worked, through the LEGAT in Manila, with the Philippines' National Bureau of Investigation, to identify the perpetrator. The investigation in the Philippines was hampered by the lack of a specific computer crime statute. Nevertheless, Onel de Guzman was charged on June 29, with fraud, theft, malicious mischief, and violation of the Devices Regulation Act. The speed with which the virus was traced back to its source is unprecedented. As a postscript, it is important to note that the Philippines' government on June 14, 2000 approved the E-Commerce Act, which now specifically criminalizes computer hacking and virus propagation.

In addition to the matters mentioned above, we are currently working on numerous cases that require international cooperation. Because these are all pending matters, I cannot comment on them in this hearing. But I can say that the percentage of cases with an international element is increasing significantly.

These cases all illustrate the tremendous progress that has been made in the

international arena. Countries around the world are addressing the cyber crime problem by creating new computer crime laws, establishing organizations and capabilities to handle investigations, and forging ties across international borders to facilitate investigations. While much work remains to be done, we can point with pride to the considerable advances that have been made in a very short time to strengthen international cooperation against cyber crime.

Conclusion

Cooperation among governments and between government and industry is the key to combating crime in cyberspace and making the Internet a safe and secure environment for e-commerce and communications. The NIPC has played an important role in fostering such cooperation. With the support of this committee and Congress as a whole, we hope to continue to build on this success.

Thank you.

[12000 Congressional Statement](#) | [FBI Press Room](#) | [FBI Home Page](#) |

APPENDIX B

PRESIDENTIAL DECISION DIRECTIVE 39 (UNCLASSIFIED)

The following is a copy of an unclassified* abstract derived from Presidential Decision Directive (PDD-39)/U.S. Policy on Counterterrorism, dated June 21, 1995. This abstract has been reviewed and approved by the National Security Council (NSC) for distribution to Federal, State, and local emergency response and consequence management personnel to assist them in responding to terrorist emergencies.

* The full text of PDD-39 is a CLASSIFIED document. State and local officials, however, should understand that PDD-39 essentially gives the responsibility of response to terrorist attacks to the FBI for "crisis management" and FEMA for "consequence management." State and local agencies and assets will be expected to support the Federal efforts.

U.S. POLICY ON COUNTERTERRORISM

Presidential Decision Directive (PDD-39)

1. **General.** Terrorism is both a threat to our national security as well as a criminal act. The Administration has stated that it is the policy of the United States to use all appropriate means to deter, defeat, and respond to all terrorist attacks on our territory and resources, both people and facilities, wherever they occur. In support of these efforts, the United States will:

Employ efforts to deter, preempt, apprehend, and prosecute terrorists.

Work closely with other governments to carry out our counterterrorism policy and combat terrorist threats against them.

Identify sponsors of terrorists, isolate them, and ensure they pay for their actions.

Make no concessions to terrorists.

2. **Measures to Combat Terrorism.** To ensure that the United States is prepared to combat terrorism in all its forms, a number of measures have been directed. These include reducing vulnerabilities to terrorism, deterring and responding to terrorist acts, and having capabilities to prevent and manage the consequences of terrorist use of nuclear, biological, and chemical (NBC) weapons, including those of mass destruction.

a. **Reducing Vulnerabilities.** In order to reduce our vulnerabilities to terrorism, both at home and abroad, all department/agency heads have been directed to ensure that their personnel and facilities are fully protected against terrorism. Specific efforts that will be conducted to ensure our security against terrorist acts include the following:

Review the vulnerability of government facilities and critical national infrastructure.

Expand the program of counterterrorism.

Reduce the vulnerabilities affecting civilian personnel/facilities abroad and military personnel facilities.

Exclude/deport persons who pose a terrorist threat.

Prevent unlawful traffic in firearms and explosives, and protect the President and other officials against terrorist attack.

Reduce U.S. vulnerabilities to international terrorism through intelligence collection/analysis, counterintelligence, and covert action.

b. **Deter.** To deter terrorism, it is necessary to provide a clear public position that our policies will not be affected by terrorist acts and we will vigorously deal with terrorist sponsors to reduce terrorist capabilities and support. In this regard, we must make it clear that we will not allow terrorism to succeed and that the pursuit, arrest, and prosecution of terrorists is of the highest priority. Our goals include the disruption of terrorist-sponsored activity including termination of financial support, arrest and punishment of terrorists as criminals, application of U.S. laws and new legislation to prevent terrorist groups from operating in the United States, and application of extraterritorial statutes to counter acts of terrorism and apprehend terrorists outside of the United States. Return of terrorists overseas, who are wanted for violation of U.S. law, is of the highest priority and a central issue in bilateral relations with any state that harbors or assists them.

c. **Respond.** To respond to terrorism, we must have a rapid and decisive capability to protect Americans, defeat or arrest terrorists, respond against terrorist sponsors, and provide relief to the victims of terrorists. The goal during the immediate response phase of an incident is to terminate terrorist attacks so that the terrorists do not accomplish their objectives or maintain their freedom, while seeking to minimize damage and loss of life and provide emergency assistance. After an incident has occurred, a rapidly deployable interagency Emergency Support Team (EST) will provide required capabilities on scene: a Foreign Emergency Support Team (FEST) for foreign incidents and a Domestic Emergency Support Team (DEST) for domestic incidents. DEST membership will be limited to those agencies required to respond to the specific incident. Both teams will include elements for specific types of incidents such as nuclear, biological, or chemical threats.

The Director, FEMA, will ensure that the Federal Response Plan is adequate for consequence management activities in response to terrorist attacks against large U.S. populations, including those where weapons of mass destruction are involved. FEMA will also ensure that State response plans and capabilities are adequate and tested. FEMA, supported by all Federal Response Plan signatories, will assume Lead Agency role for consequence management in Washington, DC and on scene. If large scale casualties and infrastructure damage occur, the President may appoint a Personal Representative for consequence management as the on scene Federal authority during recovery. A roster of senior and former government officials willing to perform these functions will be created and the rostered individuals will be provided training and information necessary to allow them to be called on short notice.

Agencies will bear the costs of their participation in terrorist incidents and counterterrorist operations, unless otherwise directed.

d. **NBC Consequence Management.** The development of effective capabilities for preventing and managing the consequences of terrorist use of nuclear, biological, or chemical (NBC) materials or weapons is of the highest priority. Terrorist acquisition of weapons of mass destruction is not acceptable and there is no higher priority than preventing the acquisition of such materials/weapons or removing this capability from terrorist groups. FEMA will review the Federal Response Plan on an urgent basis, in conjunction with supporting agencies, to determine its adequacy in responding to an NBC-related terrorist incident; identify and remedy and shortfalls in stockpiles, capabilities, or training; and report on the status of these efforts in 180 days.