Questions for the Record
June 20, 2000

Senator Kyl:

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

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

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

Doc. #14

news media. All of these mechanisms have been used numerous times (as discussed in the answer to the next question).

Senator Kyl's question goes to the heart of I&W in the cyber world: should the Nation have the capability to detect intrusions into government or private sector systems in an automated fashion, without having to rely on human detection and reporting? The controversy attending the Administration's recent "FIDNET" initiative, which is a limited proposal to place automated intrusion detection devices on federal agency networks, identified many of the privacy and other issues such a system would raise, particularly if it were extended to privately owned networks. The government's approach at the present time is to encourage industry to protect and monitor its own systems, and to report anomalous activity voluntarily. The NIPC works within that overall policy to encourage private sector reporting as a critical part of its I&W. Examples of this include InfraGard and the incident reporting pilot program we have developed with the energy sector through the North American Electrical Reliability Council (NERC).

Q: How many warnings has the NIPC issued which were developed through the Centers's own analysis of activity?

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

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

Q: What other agencies do you see playing a significant role in the area of computer crime investigations?

Cyber crime is an issue that concerns not just the FBI, and not just law enforcement generally. Indeed, "cyber crime" in itself should be seen as part of a broader array of cyber threats, including cyber terrorism, cyber espionage, and information warfare, since all are closely related and often difficult to distinguish at the outset of an incident. As a result, cyber threats are

of great concern to numerous federal agencies, including the Defense, Intelligence, and Law Enforcement Communities and to civilian "Lead Agencies" under PDD-63; to state and local governments, including law enforcement; and, of course, to the private sector. It is because of this wide-ranging interest that the NIPC was established as an interagency center. The NIPC provides a locus and mechanism for coordinating the expertise and roles of many agencies, and facilitates information sharing and operational coordination. The NIPC works closely on investigative matters with many law enforcement agencies, including: the Secret Service, Internal Revenue Service (IRS), Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), United States Air Force Office of Special Investigations (AFOSI), Defense Criminal Investigative Service (DCIS), National Aeronautics and Space Administration Office of Inspector General (NASA OIG), Department of Energy (DOE), state and local law enforcement, the Intelligence Community, as well as foreign law enforcement agencies through FBI Legal Attaches (LEGATS).

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

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

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

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has

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

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

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

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

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations

under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

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

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

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

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

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

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

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

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

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

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

Since the founding of the NIPC in February 1998, there are numerous cases which have demonstrated successful interagency cooperation other than the significant Solar Sunrise and Moonlight Maze cases. The importance of these two cases should not be overlooked, however. Both represent significant milestones in building awareness of the cyber threat among federal agencies and policymakers, demonstrated significant vulnerabilities in DoD and other government systems, and provided opportunities to test and improve the NIPC's processes for interagency coordination.

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

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

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

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

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

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

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

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

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

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

Other

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

Senator Feinstein:

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

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

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

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

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

the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

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

How would you assess progress in the case now?

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

> On February 8, 2000, the FBI received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship the NIPC has developed with the private sector, in the days that followed, several other companies also reported denial of service outages. These companies cooperated with our National Infrastructure Protection and Computer Intrusion squads in the FBI field offices and provided critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages.
>
> *The resources required in these investigations can be substantial.* Already we have five FBI field offices with cases opened: Los Angeles, San Francisco, Atlanta, Boston, and Seattle. Each of these offices has victim companies in its jurisdiction. In addition, so far seven field offices are supporting the five offices that have opened investigations. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers, and providing all-source analytical assistance to field offices. Agents from these offices are following up literally hundreds of leads. While the crime may be high tech, investigating it involves a substantial amount of traditional police work as well as technical work. For example, in addition to following up leads, NIPC personnel need to review an overwhelming amount of log information received from the victims. Much of this analysis needs to be done manually. Analysts and agents conducting this analysis have been drawn off other case work. In the coming years we expect our case load to substantially increase. (Emphases added.)

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

On February 8, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

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

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

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

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

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

3. In testimony last February 16, you suggested that the FBI's resources "are stretched paper-thin" because of the lack of high-caliber government forensic computer experts.

How much has this contributed to the government's lack of success in catching the perpetrators of the February cyber attacks?

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

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

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

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

CART Capacity and Backlog

Year	FTE Staffing	Capacity	Exam Requests	Case Backlog	Backlog Time (Months)
1999	95	1900	3500	1600	10.1
2000	104	2080	5000	2920	16.8
2001	154	3080	6000	2920	11.4
2002	213	4260	8500	4240	11.9

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

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

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

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

Meanwhile, our pending case load has grown rapidly.

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

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

Evidence gathering for computer intrusions mandates a prompt response because the digital evidence trail can disappear so quickly. The complexity of documenting, examining and analyzing the tremendous amount of information that is necessarily collected in these types of cases and its very technical nature requires investigators, examiners, and analysts with extremely

specific skills and experience. Because of the technical nature of this crime, it is difficult, if not impossible, to temporarily assign additional Special Agents to an investigation since a special technical skill set is required to investigate such matters.

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

4. Some have argued that the high-profile February attacks on Yahoo, eBay, and other companies were just a diversion, allowing the hackers to focus on making smaller, intrusive attacks on smaller sites.

Have you found any evidence for this contention?

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

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

The Internet was not designed with security as the foremost consideration. Moreover, until very recently, security was not a major priority of either hardware/software manufacturers or consumers. As a result, networks are still rife with vulnerabilities. Improving security on the Internet is thus first and foremost the responsibility of industry. Government must protect its own systems, and can assist industry by providing information about threats and vulnerabilities that we are aware of, and the NIPC does that. But it is industry's responsibility to secure privately owned systems.

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

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

The vulnerabilities that permeate the industry are a big problem for the FBI and other law enforcement agencies because they make it so easy for crimes to be committed. This accounts in

Senator Grassley

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

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

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

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

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

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

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

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

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

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

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

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of

law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

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

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

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

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

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

Other

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

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

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

how the FBI field offices make direct contact with their counterpart field offices, such as US Secret Service, to coordinate aspects of an investigation.

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

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

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

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

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

The FBI currently has one local law enforcement officer assigned to the NIPC. He is from the Tuscaloosa County Sheriffs Department and his principal job is to work on outreach initiatives

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

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

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

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

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

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

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

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

public safety and national security.

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

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

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

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

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

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

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

Senator Leahy:

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

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

in excess of $5,000.

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

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

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

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

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

The question calls for an interpretation of a statute applying the substantive case law of

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

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

The NIPC referred this question to the Department of Justice Computer Crimes and Intellectual Property Section for input. The Department reported that it could recall no cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. § 1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. § 5G1.2.

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

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

> [t]he new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal

Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

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

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

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

7. The FBI has limited authority to issue administrative subpoenas in certain cases, such as federal health care fraud or sexual exploitation or other abuse of children. Since cybercrime cases are criminal in nature, is the FBI able to obtain documents relevant to the investigation with grand jury subpoena? To the extent that documents obtained with a

---

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

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

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

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

grand jury subpoena need to be shared with third-party experts, can permission be obtained to do so under Federal Rule of Criminal Procedure 6(e)(3)?

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

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

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

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

consent to electronic surveillance? Would an exception to the wiretap law to allow the unwitting victim system operator to grant consent to electronic surveillance be helpful to law enforcement?

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

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

I. Is law enforcement currently required to obtain a wiretap in order to document in real-time the remote commands being given to a target system?

potential exception to this would be certain pen register-based approaches employed by service providers in switch-based solutions, where post-cut-through dialing (including post-cut- through signaling) may not be provided to law enforcement. This circumstance is currently a subject of review by the FCC under rule making implementing CALEA, and regarding which we anticipate a resolution in the near future.) The distinction between a pen register device on a telephony service and a clone pager (or pager interception) is that a pen register is employed to capture dialed numbers which are used to set up a call. Hence, in the overwhelming majority of instances where pen registers are used the information captured is simply signaling information used to set up a call. By comparison, pager interceptions are employed to capture the information received by a pager which, in all instances, constitute the content or message of the call. Consequently, the law has historically distinguished the legal processes required for these two types of acquisitions (i.e., pen register authority vs Title III authority, respectively).

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

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

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

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

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

under section 3122.

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

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

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

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

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

Pen Register certifications by government attorneys are drafted and filed by attorneys of the Department of Justice and not, at the Federal level, by Special Agents of the FBI. Questions regarding the substance of such certifications would more appropriately directed to the Department of Justice for a more definitive response. As a general matter, however, it is the FBI's experience that the degree to which a pen register application to the Court discloses the underlying factual basis for the attorney's certification turns, in large measure, upon the nature of the statutory offense which is the focus of the investigation. Whereas section 3123(b)(1)(D) requires that all pen register orders contain a "statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates," it follows that the application required by section 3122(b)(2) contain

such a statement within the attorney's certification and it is the FBI's experience that this is commonly the case. Depending upon the nature of the offense described in the certification, the underlying basis for the certification can, and in most instances will be readily apparent. Thus, in telemarketing fraud investigations, the obvious underlying basis is that the offenders are using the telephone to solicit victims. Similarly in narcotics and conspiracy to commit narcotics violations, the reliable and common sense inference is clearly that telecommunications are being used to facilitate the possession, distribution and sale of controlled substances in violation of Title 21 of the United States Code. Even in investigations involving computer hacking in violation of the Computer Fraud and Abuse Act (18 U.S.C. §§1030 *et seq.*), it requires little thought or imagination to understand the underlying basis for the request.

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

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

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

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

On its face, the provisions of H.R. 1714 which allow for the electronic storage of contracts, agreements and records are unrelated to earlier provisions of the bill delineating what types of legal documents may be executed by electronic signature. To the extent that Section 101(c)(1)(c) could be interpreted as allowing for the electronic imaging and storage as an electronic record of written contracts or agreement, the tangible originals of which would otherwise be required by law to be maintained in tangible form, then, there could exist the potential to negatively impact certain law enforcement investigations relating to such documents. At a minimum, the supplanting of tangible originals (otherwise legally required to be maintained in tangible form) with electronic images depicting the originals, when coupled with destruction of the originals, would eliminate or complicate handwritten signature analysis and render null the possibility of recovering fingerprints or other trace evidence from the surface of originals. By the same token, the provisions of section 101(c)(2) which exempt from retention data relating to the communication or receipt of any contract, agreement or record electronically recorded, could, in the context of electronically executed contracts, complicate or eliminate law enforcement efforts in tracing the source of transmission of fraudulent transactions or the location and identity of co-conspirators or even other victims. The continued trend toward electronic, paper-less execution of commercial transactions (which is admittedly so critical to the continued evolution and expansion of the Internet) when coupled with 1) the growing ability of criminals to utilize encryption to restrict law enforcement's ability to recover crucial inculpatory evidence, and 2) the absence of any preeminent public key, or private signature verification entity or procedure complicates the efforts of the FBI and state law enforcement to protect the public from on-line fraud.

1. synopses only of documents can negatively impact law enforcement?

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

2. If states are hindered . . .

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