Statement for the Record of Ronald L. Dick,

Director, National Infrastructure Protection Center
Federal Bureau of Investigation
Before the
Senate Committee on Governmental Affairs

May 8, 2002

Mr. Chairman, Ranking Member Thompson, and members of the committee, thank you for inviting me here today to testify on the topic, "Critical Infrastructure Information Sharing." Holding this hearing demonstrates your individual commitment to improving the security of our Nation's critical infrastructures and this committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. We have seen how a terrorist attack can have immediate simultaneous impact on several interdependent infrastructures. My testimony today will address information sharing as it relates to our mission at the National Infrastructure Protection Center. Our combined mission supports information and physical security, law enforcement, national security, and the military.

As set forth in Presidential Decision Directive 63 (PDD-63), the mission of the NIPC is to provide "a national focal point for gathering information on threats to the infrastructures" and to provide "the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." The Directive defines critical infrastructures to include "those physical and cyber-based systems essential to the minimum operations of the economy and government," to include, without limitation, "telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." To accomplish this mission, we have had to build a coalition of trust, one . . . amongst all government agencies, two . . . between the government and the private sector, three . . . amongst the different business interests within the private sector itself, and four . . . in concert with the greater international community. Once trust has been earned, true two-way information sharing can occur. The NIPC shares information across the public and private sectors through several programs and mechanisms, with a focus on cyber security.

SHARING INFORMATION WITH FEDERAL AGENCIES, STATE AND LOCAL LAW ENFORCEMENT AUTHORITIES, THE PRIVATE SECTOR, AND INTERNATIONALLY

OVERALL NIPC INFORMATION SHARING EFFORTS

The NIPC routinely shares information with the public and private sectors to help them better protect themselves. That does not mean that information is broadcast across the news media in every instance. While public statements are the best alternative in some cases, in other cases the NIPC has approached victim companies or government agencies privately. In many cases a tiered approach is taken so that information with the appropriate level of detail reaches the right audiences. If the NIPC finds that despite issuing an advisory, a widespread problem persists or grows, then an advisory may be reissued.

The NIPC has a variety of information products to inform the private sector and other domestic and foreign government agencies of the threat, including: assessments, advisories and alerts; a *Daily Report*; biweekly *CyberNotes*; monthly *Highlights*; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, *Highlights* is a monthly publication for sharing analysis and information on critical infrastructure issues. It provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in an unclassified format and reaches national security and civilian government agency officials as well as infrastructure owners. *CyberNotes* is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published twice a month on the NIPC website (www.nipc.gov(www.nipc.gov)) and disseminated via e-mail to government and private sector recipients.

Although the NIPC can and does issue limited distribution products that are classified or law enforcement sensitive (for example, because they reflect non-public sources and methods), it attempts to issue most reports at the unclassified level and to the widest audience possible.

To better share information, the NIPC has spearheaded an aggressive outreach effort. NIPC officials have met with business, government, and community leaders across the United States and around the world to build the trust required for information sharing. Protection of business information and privacy interests are both stressed in NIPC internal deliberations and with business, government and community leaders. Most have been receptive to information sharing and value the information received from the NIPC. Others have expressed reservations due to a lack of understanding or perhaps confidence in the strength of the disclosure exceptions found in the Freedom of Information Act, concerns about whether the Justice Department would pursue prosecutions at the expense of private sector business interests, and simple reluctance to disclose proprietary information to any entity beyond their own control or beyond the direct control of the NIPC.

The annual Computer Security Institute/FBI Computer Crime and Security Survey, released in April, indicated that 90% of the respondents detected computer security breaches in the last 12 months. Only 34% reported the intrusions to law enforcement. On the positive side, that 34% is more than double the 16% who reported intrusions in 1996. The two primary reasons for not making a report were negative publicity and the recognition that competitors would use the information against them. Many respondents were not aware that they could report intrusions to law enforcement. We have moved aggressively to address these concerns and go out of our way to reassure businesses that their voluntarily provided information will remain secure, and that we are always sensitive to protecting the interests of victims who report crime.

WATCH AND WARNING

The NIPC Watch maintains a round-the-clock presence in the FBI's Strategic Information and Operations Center (SIOC). The Watch serves as the main portal into and out of the NIPC. Our recent advisory regarding the Klez.h worm was issued after the Watch received a voluntary report from a major telecommunications company. Following an analysis and consultations with our security partners, the NIPC issued Alert 02-2002: "W32/Klez.h @ mm Worm and Variants." Through the Watch, the Center produces and disseminates three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National Threat Warning System. Collectively, these warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact. If a particular warning is based on classified material that includes dissemination restrictions and contains information deemed valuable and essential for critical infrastructure protection, the NIPC will then seek to develop a sensitive "tear-line" version for distribution, including to critical sector coordinators, InfraGard members, and general law enforcement authorities. The three specific categories of NIPC warning products are as follows:

(1) "Assessments" address broad, general incident or issue awareness information and analysis that is both significant and current but does not necessarily suggest immediate action.

(2) "Advisories" address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

(3) "Alerts" address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

The main "audiences" that NIPC products can reach include: DoD, Federal civil agencies, the Intelligence Community, the Law Enforcement Community (including the state and local levels), FBI field offices and international Legal Attache offices, computer incident response centers, domestic and foreign cyber watch centers, private sector Information Sharing and Analysis Centers (ISACs), InfraGard members (see below for an explanation of the InfraGard program), and the general public.

Since its inception, the NIPC has issued over 100 warning products. A number of warning products have

preceded incidents or prevented them entirely by alerting the user community to a new vulnerability or hacker exploit before acts are committed or exploits are used on a widespread basis. The Center has had particular success in alerting the user community to the presence of Denial of Service tools on the network and has in some cases provided a means to discover the presence of tools on a network. For example, in December 1999, as part of our Y2K efforts, the NIPC released a warning message along with a tool to allow users to find the presence of three specific denial of service tools on their systems. This was something never before done by the government for the user community and occurred over a month before the Distributed Denial of Service Attacks of February, 2000. The NIPC's work with private companies has been so well received that the Systems Administrators and Network Security Organization (SANS-a trade group) awarded their yearly Security Technology Leadership Award to members of the NIPC's Special Technologies Applications Unit.

The NIPC is integrated into national level warning systems both through structures established by the National Security Council and by other agencies. Of particular note is the fact that the NIPC has been fully engaged in the planning and implementation of the interagency Cyber Warning Information Network (CWIN). Also of note: the NIPC, under the authority of the FBI, is the only locus where the widest range of law enforcement, counterintelligence, foreign intelligence, and private sector information may be lawfully collected, analyzed, and disseminated, all under well-developed statutory protections and the oversight of the Department of Justice. NIPC Advisory 01-003 and its companion NIPC Advisory 00-060, issued on March 8, 2001 and December 1, 2000, respectively, both on e-commerce vulnerabilities, are examples of warnings which effectively combine law enforcement, intelligence, and private sector information with the NIPC's warning mission. These advisories, coupled with a press conference on March 8, 2001, stopped over 1600 attempted exploitations by hackers. The advisories reflect the balance of information dissemination to the public with an ongoing law enforcement investigation, achieving both goals in the public's interest.

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT

With respect to sharing information within the government, PDD-63 mandates that government agencies will share information with the NIPC. The NIPC has established effective information sharing relationships across the U.S. Government. These arrangements are not always codified in formal interagency agreements or Memoranda of Understanding, but the important point is that they are working. The NIPC has also formed an Interagency Coordination Cell (IACC) at the Center which holds monthly meetings regarding ongoing investigations. To date, the IACC's growing membership has risen to approximately 35 government agencies that meet on a monthly basis to include representation from NASA , U.S. Postal Service, Air Force Office of Special Investigations (AFOSI), U.S. Secret Service, U.S. Customs, Departments of Energy, State and Education, and the Central Intelligence Agency, to name a few.

The IACC's accomplishments to date include the formation of several joint investigative task forces with member agencies participating, and over 30 separate instances of joint investigations of member agencies being initiated as a direct result of IACC meetings, information sharing and participation. In one case, an IACC member agency provided timely sensitive source information to the appropriate authorities which prevented the planned intrusion and compromise of another government agency's computer system and the preservation of critical log data used for the ensuing investigation.

The IACC's members are currently working on the establishment and development of a database which would serve as a source of computer intrusion information compiled from member agency investigations to facilitate other investigations. It is also working on the establishment and administration of a dedicated virtual private secure network for member agencies to communicate vital infrastructure protection and computer intrusion information for immediate emergency response situations, in addition to dissemination of routine but sensitive information.

The Department of Defense has the second largest (after FBI) interagency contingent in the NIPC. The Deputy Director of the NIPC is a two-star Navy Rear Admiral; the Executive Director is detailed from the Air Force Office of Special Investigations; the Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service; the head of the NIPC Watch is a Naval Reserve officer; and the head of the Analysis and Information Sharing Unit is a National Security Agency detailee. There are also liaison representatives from the National Imagery and Mapping Agency and the Joint Programs Office. A contingent of DoD reservists serves in the Center to provide additional critical infrastructure expertise and emergency surge capabilities. NIPC works particularly closely with

the DoD through liaison with the Joint Task Force-Computer Network Operations (JTF-CNO). NIPC members stay in close contact with their JTF-CNO counterparts, providing mutual assistance on intrusion cases into DoD systems, as well as on other matters. NIPC alerts, advisories, and assessments are routinely coordinated with the JTF-CNO prior to release to solicit JTF input. On several occasions, the NIPC and JTF-CNO have coordinated and issued joint cyber warnings on the same matter. There is also significant interaction with the military services, the Joint Staff, the Office of the Secretary, and other major DoD agencies.

Interagency managerial participation is by no means limited to DoD. For example, the Section Chief for Analysis and Warning is detailed from the Central Intelligence Agency, and the Assistant Section Chief for Computer Investigations and Operations is detailed from the U.S. Secret Service.

The NIPC also has an excellent cooperative relationship with the Federal Computer Incident Response Center (FedCIRC). The FedCIRC has detailed a person to our Watch Center in the past, and the NIPC's Director sits on FedCIRC's Senior Advisory Council. FedCIRC is operated by the General Services Administration as the central coordinating point on security vulnerabilities and lower level security incident data. In addition, the NIPC sends draft alerts, advisories, and assessments on a regular basis to FedCIRC for input and commentary prior to their release. NIPC and FedCIRC information exchange assists both centers with their analytic products. The NIPC and FedCIRC are currently discussing ways to improve the flow of information between the two organizations and encourage federal agency reporting of incident information. On several occasions, the two organizations have coordinated and issued joint cyber warnings.

More recently, in October of 2001, President Bush issued Executive Order 13231, which establishes the President's Critical Infrastructure Protection Board to "recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems." EO 13231 expressed the current Administration's continued support of the NIPC's mission under PDD 63 and distinguishes the interagency entity from any particular Department by separately designating the Director of the NIPC to serve as a member of the newly created President's Board. The President also designated the Director of the NIPC to serve on the Board's Coordination Committee, together with only the Director of the Critical Infrastructure Assurance Office (Commerce); the Manager of the National Communications Systems (DoD); the Vice Chair, Chief Information Officers' (CIO) Council, NSA; and the Deputy Director of Central Intelligence for Community Management. Also of significance, President Bush specified within EO 13231 that the Board must work in coordination with the NIPC in connection with the following activities: (1) Outreach to the Private Sector and State and Local Governments; (2) Information Sharing; (3) Incident Coordination and Crisis Response; and (4) Law Enforcement Coordination with National Security Components.

Since 1998, the NIPC has been developing the FBI’s Key Asset Initiative, to identify those entities that are vital to our national security, including our economic well-being. The information is maintained to support the broader effort to protect the critical infrastructures against both physical and cyber threats. This initiative benefits national security planning efforts by providing a better understanding of the location, importance, contact information and crisis management for critical infrastructure assets across the country. We have worked with the DoD and the Critical Infrastructure Assurance Office (CIAO) in this regard.

INTERAGENCY COORDINATION: FEDERAL, STATE AND LOCAL

Emergency Law Enforcement Services Sector

The NIPC has been designated by the Department of Justice/FBI to fulfill their responsibilities as the Sector Lead Agency with regard to Emergency Law Enforcement Services (ELES). The NIPC's efforts in this regard have served as a model for all other Sector Lead Agencies. More than 18,000 federal, state and local agencies comprise the ELES Sector. The NIPC serves as program manager for this function at the request of the FBI. Last year the NIPC completed the Emergency Law Enforcement Services Sector Plan; this was the first completed sector report under PDD-63 and was delivered to the White House in March 2001. Working with law enforcement agencies across the United States, the NIPC conducted a sector survey and used the results of this survey to draft a sector report. Responses from more than 1500 of

these agencies to a sector-commissioned information systems vulnerability survey revealed that these organizations have become increasingly reliant on information and communications systems to perform their critical missions. The NIPC has also sponsored the formation of the Emergency Law Enforcement Services Sector forum, which meets quarterly to discuss issues relevant to sector security planning.

State Infrastructure Protection Center (SIPC) efforts

The NIPC, with its extensive experience in the areas of multi-agency and multi-disciplinary support to infrastructure protection efforts, is actively engaged in supporting similar models being created at the state and local level. The State of Texas has demonstrated itself as a leader in this area, and the NIPC, together with significant Department of Defense involvement, is actively facilitating their efforts. Over time, the NIPC expects to meet the challenge of serving as the US hub for infrastructure protection efforts not only in terms of full Federal government support, but also in terms of bringing together State and Local governments for a fully coordinated national response.

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT AND THE PRIVATE SECTOR

Infragard: The Most Extensive Network of Federal and Private Sector Partners in the World for Protecting the Infrastructure

The InfraGard program is a nationwide initiative that grew out of a pilot program started at the Cleveland FBI field office in 1996. Today, all 56 FBI field offices have active InfraGard chapters. Nationally, InfraGard has over 4000 members. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service the FBI provides to InfraGard members free of charge. It particularly benefits small businesses which have nowhere else to turn for assistance. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The InfraGard program received the 2001 World Safe Internet Safety Award from the Safe America Foundation for its efforts.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. InfraGard provides a mechanism for the public and private sectors to exchange information pertaining to cyber intrusion matters, computer network vulnerabilities and physical threats on infrastructures. All InfraGard participants are committed to the proposition that the exchange of information about threats on these critical infrastructures is an important element for successful infrastructure protection efforts. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

Private sector members and an FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership. The chapter members include representatives from the FBI, State and local law enforcement agencies, other government entities, private industry and academia. The National Infrastructure Protection Center and the Federal Bureau of Investigation play the part of facilitator by gathering information and distributing it to members, educating the public and members on infrastructure protection, and disseminating information through the InfraGard network.

InfraGard is responsible for providing four basic services to its members: secure and public WebSites, an alert and incident reporting network, local chapter activities, and a help desk. Under this program the FBI provides a secure electronic communications capability to all InfraGard members so that the NIPC can provide threat information to private industry owners and operators, and encourage private industry coordination with law enforcement, and each other, on cyber and related physical incidents. This will be accomplished by expanding the established separate WebSite and

electronic mail system. The program anticipates at least 100 members in each chapter with further expansion as the program develops, with approximately 2,500 new members expected in calendar year 2002. A number of the larger field divisions anticipate starting several chapters in larger cities located in their respective geographic area of responsibility. The warnings that are provided to our InfraGard members improve the relationship between private industry and the local FBI offices due to the increased level of trust that is often established. It should be noted that the InfraGard program is not responsible for producing the alerts and warnings that are disseminated from the NIPC.

Information Sharing and Analysis Centers (ISACs)

The NIPC is continuing to reach out to the Information Sharing and Analysis Centers (ISACs). The NIPC has recently initiated the establishment of an ISAC Support and Development Unit, whose mission is to enhance private sector cooperation and trust, resulting in two-way sharing of information and increased security for the nation's critical infrastructures. The NIPC now has information sharing agreements with seven ISACs, including those representing energy, telecommunications, information technology, air transportation, water supply, food, and chemical sectors. Several more agreements are in the final stages. Just as important, the NIPC is receiving reports from member companies of the ISACs. The NIPC has proven to these companies that it can properly safeguard their information and can provide them with useful information. It is because of such reporting that the investigative caseload of the NIPC is burgeoning and more analytical products are being issued each year.

One example bears discussion. The North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC for an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information and the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. Additionally, some information available to the NIPC may be classified or law enforcement sensitive and, thus, unavailable to many in the industry. A group of NERC officials have been granted security clearances in order to access classified material on a need-to-know basis. Once the NIPC has determined that a warning should be issued, cleared electric power experts will be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide members of the industry with unclassified, nonproprietary, timely and actionable information to the maximum extent possible.

CERT/CC (a federally funded research and development corporation)

The NIPC and the Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Mellon University have formed a mutually beneficial contractual relationship. The NIPC receives information from the CERT (including advance Special Communications about impending CERT advisories, which CERT seeks NIPC input on, and weekly intrusion activity information) that it incorporates into strategic and tactical analyses and utilizes as part of its warning function. The NIPC's Watch and Analysis units are routinely in telephonic contact with CERT/CC and the anti-virus community for purposes of sharing vulnerability and threat information on a real-time basis. CERT/CC input is often sought when an NIPC warning is in production. The NIPC also provides information to the CERT that it obtains through investigations and other sources, using CERT as one method for distributing information to security professionals in industry and to the public. The Watch also provides the NIPC Daily Report to the CERT/CC via Internet e-mail. On more than one occasion, the NIPC provided CERT with the first information regarding a new threat, and the two organizations have often collaborated in disseminating information about incidents and threats.

INTERAGENCY COORDINATION: FEDERAL GOVERNMENT AND INTERNATIONAL PARTNERS

The ability of the United States to assure homeland security clearly relies on the full participation and support of its international partners. It is with this in mind that the NIPC has promoted a wide array of international initiatives.

On the information infrastructure side of the equation, a typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Even intrusions into U.S. systems by a perpetrator operating within the U.S. often require international investigative activity because the attack is routed through Internet Service Providers and computer networks located outside the United States. When evidence is located within the United States, the NIPC coordinates law enforcement efforts which might include: subpoenaing records by FBI agents, conduct of electronic surveillance, execution of search warrants, seizing and examining of evidence. We can not do those things ourselves to solve a U.S. criminal case overseas. Instead, we must depend on the local authorities to assist us. This means that effective international cooperation is essential to our ability to investigate cyber crime. The FBI's Legal Attaches (LEGATs) provide the means to accomplish our law enforcement coordination abroad, and are often the first officials contacted by foreign law enforcement should an incident occur overseas that requires U. S. assistance. NIPC personnel are in almost daily contact with LEGATs around the world to assist in coordinating requests for information.

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

The NIPC is working with its international partners on several fronts. The first area consists of outreach activities designed to raise awareness about the cyber threat, encourage countries to address the threat through substantive legislation, and provide advice on how to organize to deal with the threat most effectively. The Center often hosts foreign delegations to discuss topics ranging from current cases to the establishment of NIPC-like entities in other nations. Since the NIPC was founded, Australia, Japan, Israel, the United Kingdom, Canada, Germany, South Korea and Sweden have all formed interagency entities like the NIPC. The Center has established watch connectivity with similar centers in Australia, Canada, the United Kingdom, Sweden, and New Zealand; additionally, the Canada and the United Kingdom have each detailed a person full-time to the NIPC, and Australia detailed a person for 6 months in 2001. Currently, the Center is working jointly with the Department of State to develop and implement an international strategy for information sharing in the critical infrastructure protection arena. Finally, over the past year, the NIPC has briefed visitors from the United Kingdom, Australia, Canada, Germany, France, Georgia, Norway, New Zealand, Singapore, Bulgaria, Estonia, Latvia, Japan, Denmark, Sweden, South Korea, Israel, Italy, India, and other nations regarding critical infrastructure protection issues. These nations have all looked to the NIPC in order to create Critical Infrastructure Protection Centers of their own and to promote liaison on a bi-lateral basis between themselves and the United States, as well as with one another.

At the NIPC we continue to seek partnerships which promote two-way information sharing. As Director Mueller stated in a speech on April 19th, “Our top priority is still prevention.” We can only prevent attacks on our critical infrastructures by building an intelligence base, analyzing that information, and providing timely, actionable threat-related products to our public and private sector partners. We welcome the efforts of your Committee in improving information sharing, and I look forward to addressing any questions you might have.