Statement for the Record
Michael A. Vatis
Director, National Infrastructure Protection Center
Federal Bureau of Investigation
before the
Senate Armed Service Committee,
Subcommittee on Emerging Threats and Capabilities

Washington, D. C.
March 16, 1999

Introduction

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

NIPC and PDD-63

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

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

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

The NIPC has a vital role in collecting and disseminating information from all relevant sources. Thus, the PDD directs the NIPC to Asanitize law enforcement and intelligence

information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state, and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity.@ The NIPC is also charged with issuing Aattack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators.@

In order to perform its role, the NIPC is establishing a network of relationships with a wide range of entities in both the government and the private sector. The PDD provides for this in several ways. First, it states that the Center will Ainclude representatives from the FBI, US Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, Intelligence Community and Lead Agencies.@[1] Second, the NIPC will be Alinked electronically to the rest of the government, including warning and operations centers as well as any private sector information sharing centers.@ Third, all executive departments and agencies are mandated to

[1]The lead agencies are: Commerce for information and communications; Treasury for banking and finance; EPA for water supply; Transportation for aviation, highways, mass transit, pipelines, rail, waterborne commerce; Justice/FBI for emergency law enforcement services; Federal Emergency Management Agency for emergency fire service and continuity of government; Health and Human Services for public health services. The lead agencies for special functions are: State for foreign affairs, CIA for intelligence, Defense for national defense, and Justice/FBI for law enforcement and internal security. The NIPC is performing the lead agency and special functions roles specified for AJustice/FBI@ in the PDD.

Acooperate with the NIPC and provide it assistance, information, and advice that the NIPC may request, to the extent permitted by law.@ Fourth, all executive departments are also mandated to Ashare with the NIPC information about threats and warning of attacks and actual attacks on critical government and private sector infrastructures, to the extent permitted by law.@ To ensure that the flow of information is unimpeded -- which is imperative when dealing with cyber attacks -- the PDD authorizes the NIPC to Aestablish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create.@

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

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

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

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

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

Finally, under the PDD the federal government is encouraging the creation of one or more Information Sharing and Analysis Centers (ISACs) by the private sector. As envisioned, the ISAC(s) Acould serve as a mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC.@ ISACs could also serve to further disseminate NIPC information to industry. The provision of timely and complete information to the NIPC is critical for the success of its mission, and the PDD states that the ISACs are Anot to interfere with direct information exchanges between companies and the government.@ As the government and private sector consider possible models for an ISAC, it is critical that nothing be created that would impede or delay the flow of incident and threat information to and from the NIPC. Rather, any ISAC should be designed to expedite the flow of information to enable real-time detection, analysis, and response by the NIPC.

Status of the NIPC and its Implementation of the PDD.

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

- The Computer Investigations and Operations Section (CIOS) is the operational and response arm of the Center. It program manages computer intrusion investigations conducted by FBI Field Offices throughout the country; provides subject matter experts, equipment, and technical support to cyber investigators in federal, state, and local government agencies involved in critical infrastructure protection; and provides a cyber emergency response capability to help resolve a cyber incident.

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

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

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

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

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

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

This program will be developed in coordination with DOD and other agencies. This program serves the critical needs of developing lists of the key assets within each critical infrastructure and also of developing the communications and liaison links necessary for the collection of information and the dissemination of warnings to the infrastructure owners and operators.

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

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

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

Policy and Statutory Impediments to Combating Threats to the Critical Information Infrastructure.

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

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

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

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

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

- the updating of federal trap and trace and pen register authorities in order to take account of new information technologies;

- the need for multi-jurisdictional pen register and trap and trace orders rather than multiple orders each covering one jurisdiction;

- the need to address sentencing issues regarding minors who commit computer crimes;

- the need to criminalize unauthorized computer access to sensitive computer and information networks when it is difficult to put a dollar value on the harm (since jurisdiction over many types of computer crimes currently attaches only at the $5,000 mark);

- the need to create criminal forfeiture provisions for violations of the Computer Fraud and Abuse Act, so we can seize computers of convicted computer criminals; and

- the need to clarify current law to unambiguously permit the United States to conduct domestic investigations and prosecutions when a United States computer is not itself the target of a computer crime but is used as a conduit to attack systems abroad.

Conclusion

PDD-63 established the NIPC as the operational linchpin of our efforts to protect America=s critical infrastructures in the 21st century. Ours is a national mission to combine the inputs from the government lead agencies and the private sector in order to provide analyses and warnings and to respond to an intrusion incident. But the NIPC can perform this mission only if has the necessary resources, interagency support, and information from multiple sources. I believe we have made significant progress in the first year of our existence in establishing the foundation for an effective system for preventing, detecting, and responding to cyber attacks. In just this past year, we have brought on board over 100 personnel from many agencies at NIPC HQ; established a national program for computer investigations in every FBI field office; developed and delivered advanced training in network investigations to nearly 200 FBI and other government agency investigators; developed several mechanisms and programs to share information with the private sector; begun a program to protect Akey assets@ with each infrastructure sector from cyber attack; and coordinated several national-level investigations involving numerous agencies and FBI field offices. While much as been accomplished, however, much work remains in developing our detection, prevention, warning, and response capabilities. I look forward to working with this Subcommittee and the Congress in protecting our national security against this difficult challenge.

Thank you.