United States General Accounting Office

GAO

Report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate

April 2001

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges in Developing National Capabilities

GAO-01-323

Contents

Abbreviations

AISU	Analysis and Information Sharing Unit
CERT/CC	Computer Emergency Response Team Coordination Center
CIA	Central Intelligence Agency
DOD	Department of Defense
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
GSA	General Services Administration
HHS	Department of Health and Human Services
ISAC	Information Sharing and Analysis Center
NIPC	National Infrastructure Protection Center
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PDD	presidential decision directive
SANS	Systems Administration, Networking, and Security Institute

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

April 25, 2001

The Honorable Jon Kyl
Chairman
The Honorable Dianne Feinstein
Ranking Member
Subcommittee on Technology, Terrorism,
and Government Information
Committee on the Judiciary
United States Senate

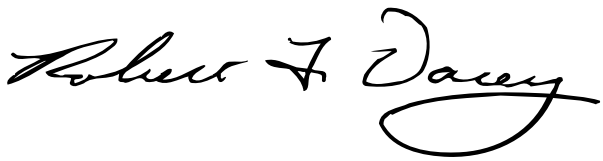
The Honorable Charles E. Grassley
United States Senate

In response to your request of May 16, 2000, this report describes the progress of the National Infrastructure Protection Center (NIPC) in (1) developing national capabilities for analyzing cyber threat and vulnerability data and issuing warnings, (2) enhancing its capabilities for responding to cyber attacks, and (3) developing outreach and information-sharing initiatives with government and private-sector entities. In addition, we were asked to determine the purposes for which the NIPC used funding provided for fiscal years 1999 and 2000.

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies to other interested congressional committees; the Honorable Condoleezza Rice, Assistant to the President for National Security Affairs; the Honorable John Ashcroft, Attorney General; the Honorable Louis Freeh, Director of the Federal Bureau of Investigation; and the Honorable Mitchell E. Daniels, Jr., Director of the Office of Management and Budget. The report will also be available on GAO's Web site at www.gao.gov.

If you or your offices have any questions about matters discussed in this report, please call me at (202) 512-3317 or Jean Boltz, Assistant Director, at (202) 512-5247. We can also be reached by e-mail at daceyr@gao.gov and boltzj@gao.gov, respectively. Major contributors to this report include

Michael Gilmore, Rahul Gupta, Danielle Hollomon, William McDaniel, Paul Nicholas, Patrick Sullivan, and Thomas Wiley.



Robert F. Dacey
Director, Information Security Issues

Executive Summary

Purpose

To address concerns about protecting the nation's critical computer-dependent infrastructures from computer-based attacks and disruption, in 1998, the President issued Presidential Decision Directive (PDD) 63. A key element of the strategy outlined in that directive was establishment of the National Infrastructure Protection Center (NIPC) as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. To determine how effectively the NIPC has fulfilled its role, the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary, asked that GAO evaluate the progress the NIPC has made in (1) developing national capabilities for analyzing threat and vulnerability data and issuing warnings; (2) enhancing its capabilities for responding to cyber attacks; and (3) developing outreach and information-sharing initiatives with government and private-sector entities, including the progress made regarding the InfraGard Program and development of the key asset database. In addition, GAO was asked to determine the purposes for which the NIPC used funding provided for fiscal years 1999 and 2000.

Background

Since the early 1990s, an explosion in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the way that the government, the nation, and much of the world communicate and conduct business. The benefits have been enormous in terms of faster communications and easier access to data. However, this widespread interconnectivity carries enormous risks to computer systems and, more importantly, to the critical operations and infrastructures they support, such as telecommunications, power distribution, national defense, and essential government services.

Malicious attacks, in particular, are a growing concern. The National Security Agency has determined that foreign governments already have or are developing computer attack capabilities, and that potential adversaries are developing a body of knowledge about U.S. systems and methods to attack them. In addition, reported incidents have increased dramatically in recent years. As a result, a clear risk exists that terrorists or hostile foreign states could launch computer-based attacks on systems supporting critical infrastructures to severely damage or disrupt national defense or vital public operations or steal sensitive data.

Concerns about computer-based vulnerabilities have been reported repeatedly during the 1990s. Since 1997—most recently in January 2001—GAO, in reports to the Congress,[1] has designated information security as a governmentwide high-risk area. In addition, in its October 1997 report,[2] the President's Commission on Critical Infrastructure Protection described, from a national perspective, the potentially devastating implications of poor information security. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats." It said that the Federal Bureau of Investigation (FBI) had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In May 1998, PDD 63 was issued in response to the commission's report. The directive called for a range of actions intended to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious computer-based attacks. The directive established a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism under the Assistant to the President for National Security Affairs. Further, the directive designated lead agencies to work with private-sector entities in each of eight industry sectors and five special functions. For example, the Department of the Treasury was responsible for working with the banking and finance sector, and the Department of Energy was responsible for working with the electric power industry. PDD 63 also authorized the FBI to expand the NIPC, which had been originally established in February 1998. The directive specifically assigned the NIPC responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to cyber incidents; providing law enforcement investigation and response; monitoring

[1] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); *High-Risk Series: An Update* (GAO/HR-99-1, January, 1999); *High-Risk Series: An Update* (GAO-01-263, January 2001).

[2] *Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection,* October 1997.

reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing.

Results in Brief

The NIPC has initiated a variety of critical infrastructure protection efforts that, together, have laid a foundation for future governmentwide efforts. However, the analytical and information-sharing capabilities that PDD 63 asserts are needed to protect the nation's critical infrastructures have not yet been achieved. The NIPC has issued numerous analyses to support investigations of individual incidents, but it has developed only limited capabilities for strategic analysis of threat and vulnerability data. Accordingly, the NIPC often is not able to provide timely information on changes in threat conditions or warnings of imminent attacks. Developing such capabilities is a formidable task, and experts say it will take an intense interagency effort to develop the related methodology. In addition, information on critical infrastructure components has not been provided to the NIPC, and the NIPC does not yet have adequate staff and technical expertise. A major underlying problem is that the NIPC's roles and responsibilities have not been fully defined and are not consistently interpreted by other entities involved in the government's broader critical infrastructure protection strategy. Further, these entities have not provided the information and support, including staff detailees, to the NIPC that were envisioned by PDD 63 and that are needed to support development of analysis and warning capabilities.

The NIPC has had greater success in providing technical support and coordination for the FBI's investigations of attacks on computer systems, which it refers to as "computer crime." In particular, the NIPC has provided valuable tools and technical assistance to the squads and teams that the FBI has established in its field offices to investigate the growing number of attacks on computer systems. In addition, it has developed procedures for establishing crisis management teams to respond to potentially serious computer-based incidents. Since 1998, seven such teams have been established to address incidents such as the Melissa virus in 1999, the transition to the year 2000, and denial-of-service attacks in February and March 2000.

Progress in establishing information-sharing partnerships between the NIPC and private-sector and government entities has been mixed. NIPC's InfraGard Program for sharing information on computer-based threats and

incidents with individual companies and organizations has enrolled over 500 members. However, of four information-sharing and analysis centers established as focal points for infrastructure sectors, only one—the electric power industry—had developed a two-way, information-sharing partnership with the NIPC at the close of GAO's review. Further, fully productive partnerships have not been established with other federal entities, most notably the Department of Defense and the Secret Service, which also collect and analyze data on computer-based threats and vulnerabilities.

In accordance with congressional direction, the NIPC obligated about $24 million and about $27 million for fiscal years 1999 and 2000, respectively, according to GAO's analysis of data provided by the FBI and the NIPC. The NIPC reportedly used about 84 percent of these amounts to develop analysis and warning, investigative support, and outreach and information-sharing capabilities at the NIPC's Washington, D.C., office. The remainder of the funds was used to support computer crime investigations conducted at FBI field offices.

GAO is making a variety of recommendations to the Assistant to the President for National Security Affairs and the Attorney General regarding the need to more fully define the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with private-sector and federal entities.

Principal Findings

Multiple Factors Have Limited Progress in DevelopingAnalysis and Warning Capabilities

PDD 63 assigns the NIPC responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities as well as timely warnings of potential and actual attacks. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent.

Since its establishment in 1998, the NIPC has issued a variety of analytical products, including 15 situation reports for law enforcement investigations and a variety of publications. Most of these have been tactical analyses

pertaining to individual incidents. Strategic analysis to determine the potential broader implications of individual incidents has been limited. Such analysis would assist in evaluating the risks associated with possible future incidents and allow for effective mitigating actions and proactive risk management.

Three factors have hindered the NIPC's ability to develop strategic analytical capabilities. First, there is no generally accepted methodology for analyzing strategic cyber-based threats. For example, there is no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources. Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise. For example, the Chief of the Analysis and Warning Section position, which was to be filled by the Central Intelligence Agency, was vacant for about half of the NIPC's 3-year existence. In addition, the NIPC has been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities. Third, the NIPC does not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of GAO's work, only three industry assessments had been partially completed, and none had been provided to the NIPC.

To provide a warning capability, the NIPC established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. Since 1998, the unit has issued 81 warnings and related products, many of which were posted on the NIPC's Internet Web site. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. The NIPC's ability to issue warnings promptly is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

Evaluating the NIPC's progress in developing analysis and warning capabilities is difficult because the federal government's strategy and related plans for protecting the nation's critical infrastructures from computer-based attacks, including the NIPC's role, are still evolving. As a result,

- the entities involved in the government's critical infrastructure protection efforts do not share a common interpretation of the NIPC's roles and responsibilities;
- the relationships between the NIPC, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council are unclear regarding who has direct authority for setting NIPC priorities and procedures and providing NIPC oversight;
- the NIPC's role has not been formally recognized as part of national security warning procedures, which provide a means of alerting the most senior federal officials, including the President, of serious or imminent threats to national security; and
- the NIPC and the defense and intelligence communities have not developed (1) criteria for determining when a computer-based attack should be treated as a national security event, rather than as a crime, and (2) protocols for placing the NIPC in a support role, rather than a lead role, should such a national security event occur.

An additional impediment to evaluating the NIPC's progress is that the NIPC's plans for further developing its analytical and warning capabilities are fragmented and incomplete. As a result, there are no specific priorities, milestones, or program performance measures to guide NIPC actions or to provide a basis for evaluating its progress.

At the close of GAO's review, in February 2001, the National Coordinator said that the administration had begun to consider options for adjusting the federal strategy for critical infrastructure protection originally outlined in PDD 63, including provisions related to the development of analytical and warning capabilities currently assigned to the NIPC. He said that one intent of any such adjustments would be to clarify roles and responsibilities in this area.

On the basis of the criteria provided in PDD 63 and related plans, GAO recommends that the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategic analysis of computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and
- clearly define the role of the NIPC in relation to other government and private-sector entities.

In addition, GAO recommends that the Attorney General task the FBI Director to require the NIPC Director to develop a comprehensive written plan for establishing analysis and warning capabilities.

The NIPC Has Provided Valuable Investigation and Response Support

The NIPC has provided coordination and technical support to FBI field offices, which have established special squads and teams and one regional task force to address the growing number of computer crime cases. As of December 31, 2000, the FBI had established such squads, each consisting of approximately 8 FBI agents, in 16 of the FBI's 56 field offices. In addition, 40 smaller teams of from 1 to 5 agents, dedicated to working computer crime cases, had been established in the remaining FBI field offices. The number of agents assigned to NIPC squads and teams increased from 76 agents in 1998 to approximately 200 agents for fiscal years 1999 and 2000.

While the NIPC provides support, the NIPC squads are under the field offices' direct supervision. Accordingly, the field offices determine when a case is to be opened and whether an incident needs to be referred to other federal, state, or local law enforcement entities. Generally, the NIPC becomes involved when notified by the field squads through case-initiation paperwork or requests for technical assistance.

The NIPC has coordinated and supported computer crime investigations by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases; (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks; and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for each of the NIPC field squads and teams.

While these efforts have benefited the FBI's investigation efforts, insufficient computer capacity and data transmission capabilities are limiting the NIPC's ability to perform technical analyses promptly. In addition, FBI field offices are not yet providing the NIPC with the comprehensive information that officials say is needed to facilitate prompt identification and response to cyber incidents. The NIPC has developed budget requirements and performance measures to address these problems.

The NIPC also has developed crisis management capabilities to support a multiagency response to the most serious incidents from the FBI's Washington, D.C., Strategic Information Operations Center. Since 1998, seven crisis action teams have been activated to address potentially serious incidents and events, such as the Melissa virus in 1999 and the days surrounding the transition to the year 2000, and related procedures have been formalized. In addition, the NIPC has developed a draft emergency law enforcement plan to guide the response of federal, state, and local entities. As of mid-February 2001, the draft plan was being reviewed by law enforcement sector members.

PDD 63 also requires the NIPC to develop capabilities to "monitor reconstitution" of minimum required capabilities after an infrastructure attack. However, NIPC officials told GAO that they have not planned or taken any action in this regard because specific expectations for meeting the requirements briefly mentioned in PDD 63 and the *National Plan for Information Systems Protection* have not been further defined. As a result, while the NIPC has established procedures for crisis management teams, previously discussed, it is not clear what responsibilities these teams would have regarding any reconstitution efforts that may be needed as the result of a seriously damaging attack.

The National Coordinator agreed that the NIPC's specific role in this area was not clear and said that this issue would probably be addressed as the administration reviews the government's critical infrastructure protection strategy and the specific requirements for the NIPC.

GAO recommends that the Attorney General direct the FBI Director to direct the NIPC Director to (1) ensure that the NIPC has access to needed computer and communications resources, (2) monitor implementation of new performance measures to ensure that FBI field offices fully report information on potential computer crimes to the NIPC, and (3) complete development of the emergency law enforcement plan. In addition, GAO

recommends that the Assistant to the President for National Security Affairs define the NIPC's responsibilities for monitoring reconstitution.

Mixed Progress in Establishing Information-Sharing Relationships

Information sharing and coordination among private-sector and government organizations are essential to thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as GAO testified in July 2000,[3] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

NIPC efforts to establish information-sharing relationships with private organizations have met with mixed success, as shown in the following examples:

- A two-way, information-sharing partnership has developed with only one—the electric power industry—of the four information-sharing and analysis centers that have been established as focal points for infrastructure sectors. The NIPC's dealings with two of the other three centers have primarily consisted of providing information without receiving any in return, and no procedures have been developed for more interactive information sharing. GAO cannot comment on the NIPC's information-sharing relationship with the fourth center because it was not established until mid-January 2001, just before the close of GAO's review.
- Expansion of the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, has been more successful. In January 2001, NIPC officials announced that 518 organizations had enrolled in the program. GAO did not survey InfraGard members and, therefore, cannot comment on their satisfaction with the program. However, NIPC officials view InfraGard as an important step in building trust relationships with the private sector.
- The NIPC and the FBI have made only limited progress in developing a database of the most important components of the nation's critical infrastructures, referred to as the Key Asset Initiative. While FBI field offices have identified over 5,000 key assets, they had not yet been successful in obtaining the agreement of the industry sectors

[3] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation* (GAO/T-AIMD-00-268, July 26, 2000).

responsible for these assets. In addition, the Key Asset Initiative is not being coordinated with other similar federal efforts at the Departments of Defense and Commerce.

Further, the NIPC and other government entities have not established fully productive information-sharing and cooperative relationships. Federal agencies have not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget's Deputy Director for Management, directs agencies to report such information to the General Services Administration's Federal Computer Incident Response Capability. NIPC and Defense officials agree that their information-sharing procedures need improvement, noting that protocols for reciprocal exchanges of information have not been established. In addition, the expertise of the Secret Service regarding computer crime has not been integrated into NIPC efforts.

The NIPC has been more successful in providing training on investigating computer crime to government entities, which is an effort that it considers an important component of its outreach efforts. From 1998 through 2000, the NIPC trained about 300 individuals from federal, state, local, and international entities other than the FBI. In addition, the NIPC has advised five foreign governments that are establishing centers similar to the NIPC.

GAO recommends that the Assistant to the President for National Security Affairs (1) direct federal agencies and encourage the private sector to better define the types of information necessary and appropriate to exchange in order to combat computer-based attacks and to develop procedures for performing such exchanges, (2) initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, and (3) resolve discrepancies in requirements regarding computer incident reporting by federal agencies.

GAO further recommends that the Attorney General task the FBI Director to (1) formalize information-sharing relationships between the NIPC and other federal entities and industry sectors and (2) ensure that the Key Asset Initiative is integrated with other similar federal activities.

Funding Used for a Variety of NIPC-related Activities

In accordance with congressional direction, the FBI reportedly designated about $32 million in fiscal year 1999 and about $28 million in fiscal year 2000 for the NIPC. In addition, the FBI provided the NIPC with

administrative services, including budgeting, accounting, training, telecommunications, and facilities, at no cost to the NIPC. Other government agencies provided the NIPC with additional resources in the form of at least 39 detailees during fiscal years 1999 and 2000, who filled a variety of NIPC positions on a nonreimbursable basis. On the basis of GAO's analysis of information provided to it by the FBI and the NIPC, the NIPC obligated about 84 percent of its available fiscal years 1999 and 2000 funds. The rest of the available funds that the NIPC did not obligate were "no-year" funds that remained available for fiscal year 2001.

The NIPC reportedly used most of its fiscal years 1999 and 2000 funds for activities performed by its staff in Washington, D.C. These included analysis and warning activities, investigation of cyber incidents, and outreach and information sharing with government and private-sector entities. The NIPC used the remainder of its funds—about 16 percent—to pay for training, travel, and information technology for NIPC field squads and teams located in FBI field offices. These funds supplemented the funding for NIPC field squads' salaries and expenses that was provided by the FBI. GAO reviewed the funding information the NIPC provided for consistency; however, it did not independently verify the data on obligations or review the NIPC's related internal-control procedures.

Agency Comments and Our Evaluation

In comments on a draft of this report, the Director of the NIPC generally agreed with GAO's findings and stated that the NIPC considers it of the utmost urgency to address the shortcomings identified. The Director expressed the view that it is most important that the NIPC receive adequate staffing, particularly from the defense and intelligence communities, in order to address the lack of strategic analysis. The Director also noted the challenges associated with establishing information-sharing relationships with other organizations. Specifically, he stated that the Department of Justice and the NIPC have worked, and will continue to work, to develop effective protocols for information sharing within the bounds of each component's legal and policy structures and provide a level of certainty that shared information will be appropriately protected. He asserted that, through such protocols, information necessary for protecting infrastructures can be effectively shared on a timely basis. In addition, the Director emphasized that the NIPC had been in existence for only 3 years and that its performance should be measured in the context of its recent formation. Finally, the Director noted that GAO's draft report did not recommend a change to the basic PDD 63 framework. In this regard, he expressed the view that the FBI is the only locus where law enforcement,

counterintelligence, foreign intelligence, and private-sector information may be lawfully and collectively analyzed and disseminated, all under well-developed statutory protections and oversight of Justice.

The Director's letter did not comment on GAO's recommendations to the NIPC regarding the need to (1) develop a comprehensive integrated plan for developing analysis and warning capabilities, (2) ensure that the Special Technologies and Applications Unit has access to adequate computer and communications resources, (3) monitor implementation of new performance measures regarding field office reporting of information on potential computer crimes, (4) formalize relationships with other federal entities, and (5) ensure that the Key Asset Initiative is integrated with other similar federal activities.

The NIPC's comments reiterate many of the points made in GAO's report regarding the NIPC's accomplishments related to developing analysis and warning, investigative, and information-sharing capabilities. However, the NIPC did not comment on several key recommendations, including the need to improve cooperative relationships with other federal entities, such as Defense and the Secret Service. Establishing such cooperation is essential if the NIPC is to effectively serve as the government's focal point for analysis and warning regarding cyber threats. Also, as the NIPC Director states, GAO did not recommend a change to the basic PDD 63 framework, including changing the placement of the NIPC. GAO did not make such a recommendation because moving the NIPC from the FBI to another agency or establishing it as a stand-alone entity would not necessarily ensure that the deficiencies GAO identified would be addressed. These deficiencies, which included lack of a generally accepted methodology for strategic analysis, lack of data on infrastructure vulnerabilities and incidents, and insufficient staff resources, are problems that need to be addressed regardless of the NIPC's organizational placement.

In comments on a draft of this report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council said that the report highlighted the need for a review of the roles and responsibilities of the federal agencies involved in U.S. critical infrastructure protection support. The comments stated that our recommendations would be considered as the administration reviews federal cyber activities to determine how the critical infrastructure protection function should be organized. Regarding further development of analysis and warning capabilities, the Special Assistant to the President

noted that some functions might be better accomplished by distributing the tasks across several existing federal agencies, creating a "virtual analysis center" that would provide not only a governmentwide analysis and reporting capability, but that could also support rapid dissemination of cyber threat and warning information. The comments did not specifically address GAO's recommendations to the Assistant to the President for National Security Affairs regarding (1) defining the NIPC's responsibilities for monitoring reconstitution, (2) better defining needed information for combating cyber attacks, (3) developing a strategy for identifying assets of national significance, and (4) resolving discrepancies in guidance on computer incident reporting by federal agencies.

Comments from the NIPC and the National Security Council are printed in full in appendixes I and II, respectively.

Introduction

Since the early 1990s, an explosion in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the way that our government, nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research and government services. Financial and other business transactions can be executed almost instantaneously, and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with virtually an unlimited number of other individuals and groups. However, this widespread interconnectivity also poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support, such as telecommunications, power distribution, national defense, and critical government services.

To reduce these risks, in 1998, the President issued Presidential Decision Directive 63 (PDD 63), which describes a strategy for cooperative efforts by government and the private sector to protect critical, computer-dependent operations. A key element of this strategy is the establishment of the National Infrastructure Protection Center (NIPC) as "a national focal point" for gathering information on threats and providing the principal means of facilitating the federal government's response to computer-based incidents.

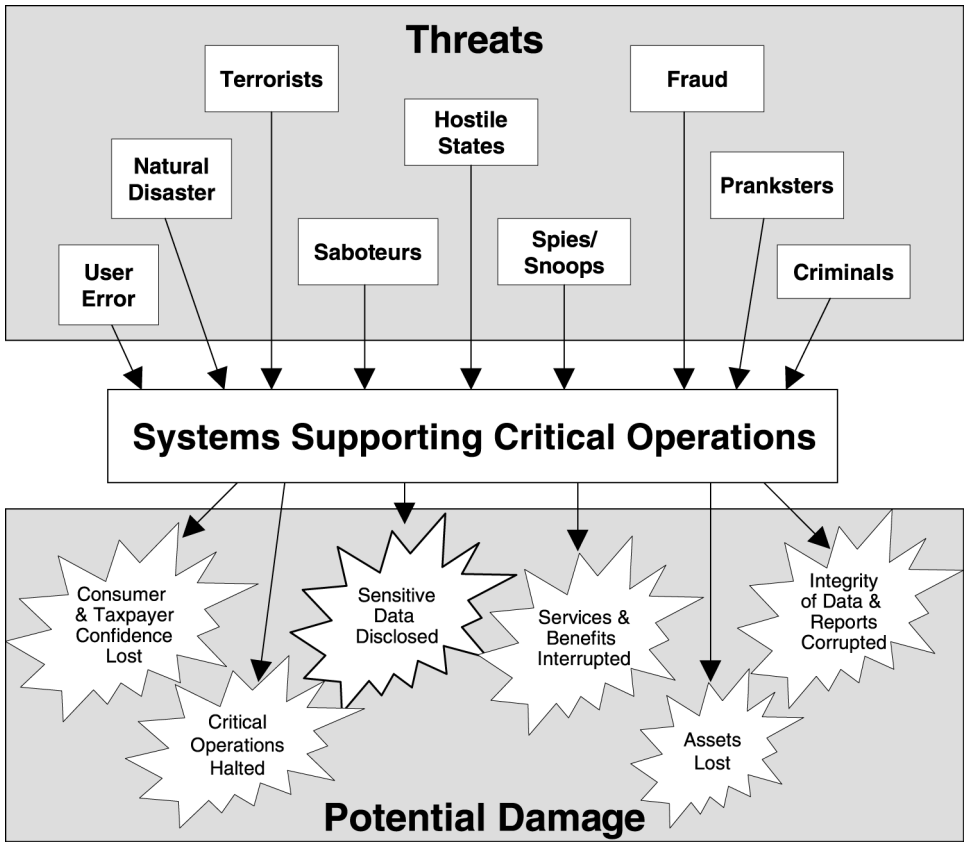
To determine how effectively the NIPC is addressing current and future cyber threats to our national security, the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary, asked that we examine the NIPC's progress in developing national capabilities for analyzing data about, issuing warnings on, and responding to computer-based attacks. In addition, the Subcommittee asked that we determine the purposes for which the NIPC used funding provided for fiscal years 1999 and 2000.

Cyber Risks to Critical Infrastructures Are Substantial and Increasing

The risks associated with our nation's reliance on interconnected computer systems are substantial and varied. Attacks can come from anywhere in the world, over the Internet, other networks, and dial-up lines. By launching attacks across a span of communications systems and computers, attackers can effectively disguise their identity, location, and intent, thereby making them difficult and time-consuming to trace.

Such attacks could severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. A significant concern is that terrorists or hostile foreign states could launch computer-based attacks on critical systems to severely damage or disrupt national defense or other critical operations or steal sensitive data, resulting in harm to the public welfare. According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems. Figure 1 provides an overview of the various types of risks.

Figure 1: Risks to Computer-Based Operations



While cyber-based attacks have not yet caused devastating disruptions, the number of attacks is increasing. Complete summary data are not available because many incidents are not reported. However, the number of reported incidents handled by Carnegie-Mellon University's CERT Coordination Center[1] has increased from about 1,300 in 1993 to about 9,800 in 1999 and to over 21,000 in 2000. Similarly, the Federal Bureau of Investigation (FBI) reports that its caseload of computer intrusion-related investigations more than doubled from 1998 to 2000. This greater number of attacks increases the risk of incidents with devastating consequences.

According to the FBI, the following threats have been observed:

Criminal groups. There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.

Foreign intelligence services. Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.

Hackers. Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.

Hacktivists. Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.

[1]Originally called the Computer Emergency Response Team, the CERT Coordination Center was established in 1988 by the Defense Advanced Research Projects Agency. The center is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.

Information warfare. Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,[2] can affect the daily lives of Americans across the country.

Insider threat. The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of victim systems often allows them to gain unrestricted access to cause damage to the system or to steal system data.

Virus writers. Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus.

Concern About Critical Infrastructure Protection Has Been Growing

Concerns about computer-based vulnerabilities have been publicly reported repeatedly during the 1990s. Examples of these concerns include the following:

- In 1991, the National Research Council studied the issue and reported that "as computer systems become more prevalent, sophisticated, embedded in physical processes and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems."[3] The report generated a great deal of interest in both the government and private sectors, alerting them to vulnerabilities and dangers being rapidly introduced with technology dependence.
- In June 1995, a Critical Infrastructure Working Group, led by the Attorney General, was formed to (1) identify critical infrastructures and assess the scope and nature of threats to them, (2) survey existing government mechanisms for addressing these threats, and (3) propose

[2]Prepared Statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

[3]*Computers at Risk: Safe Computing in the Information Age*, the National Research Council, 1991.

options for a full-time group to consider long-term government response to threats to critical infrastructures. The working group identified critical infrastructures, characterized threats to them, and recommended creating a commission to investigate such issues.

- In February 1996, the National Defense Authorization Act required the executive branch to provide a report to the Congress on the policies and plans for developing capabilities, such as warnings of strategic attacks against the national information infrastructure.[4] Later that year, the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs, began to hold hearings on security in cyberspace. Since then, congressional interest in protecting national infrastructures has remained strong.
- In July 1996, the President's Commission on Critical Infrastructure Protection was established to investigate the nation's vulnerability to both cyber and physical threats.
- Since 1997—most recently in January 2001—we have designated information security as a governmentwide high-risk area, in reports to the Congress.[5]
- In October 1997, the President's Commission issued its report,[6] which described the potentially devastating implications of poor information security from a national perspective. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats." It said that the FBI had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

[4]National Defense Authorization Act of Fiscal Year 1996*,* P. L.104-106, Div. A, Title X, Subtitle E, Section 1053.

[5]*High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); *High-Risk Series: An Update* (GAO/HR-99-1, January 1999); and *High-Risk Series: An Update* (GAO-01-263, January 2001).

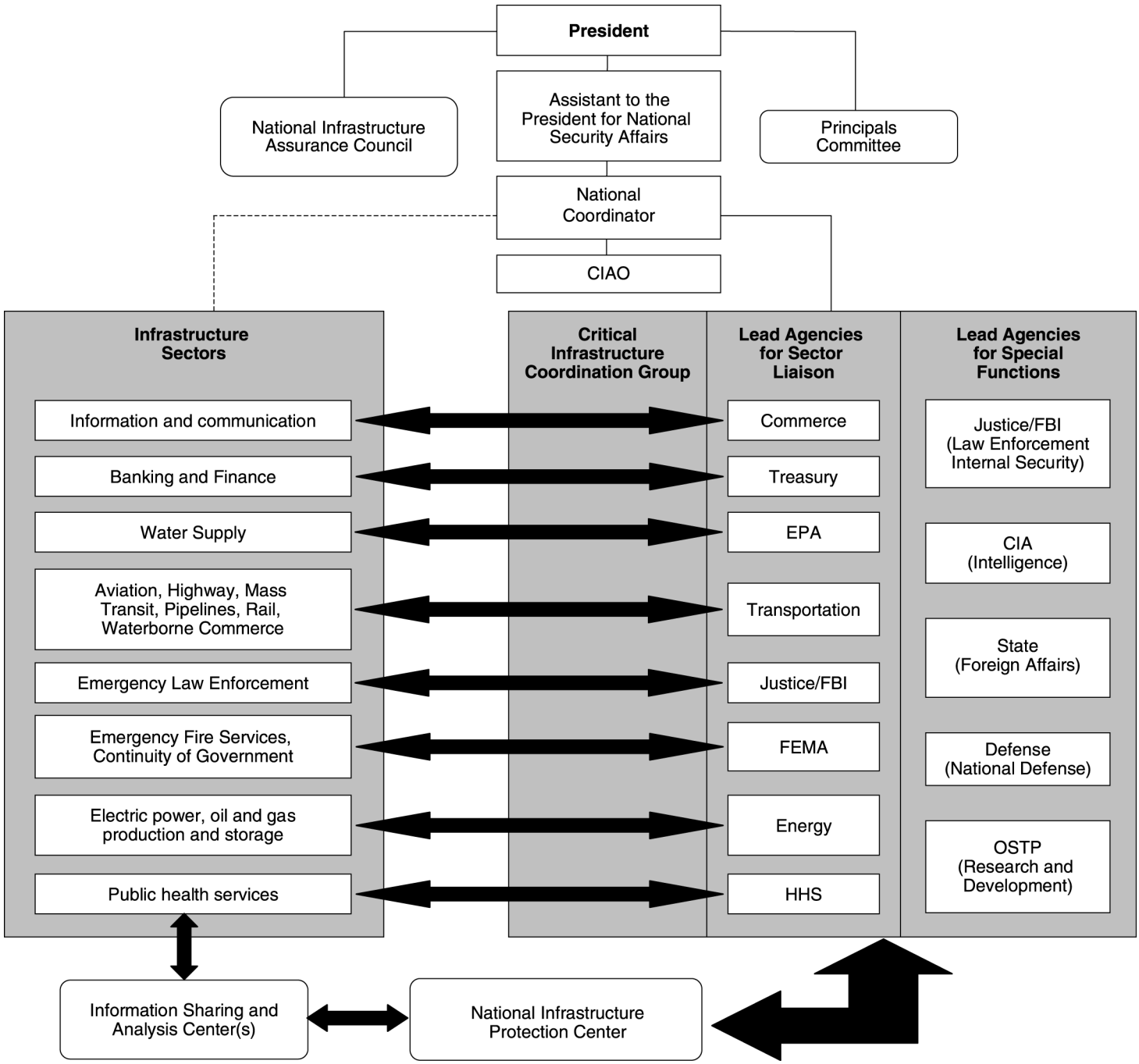
[6]*Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection,* October 1997.

PDD 63 Outlined a National Critical Infrastructure Protection Strategy

In response to the commission's report, the President initiated actions to implement a cooperative public-private approach to protecting the nation's critical infrastructures by issuing PDD 63 in May 1998. The directive called for a range of activities to improve federal agency security programs, establish a partnership between the government and private sector, and improve the nation's ability to detect and respond to serious attacks. The directive established critical infrastructure protection as a national goal, stating that, by the close of 2000, the United States was to have achieved an initial operating capability and, no later than 2003, the capability to protect the nation's critical infrastructures from intentional destructive acts.

To accomplish its goals, PDD-63 designated the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who reports to the Assistant to the President for National Security Affairs, to oversee national policy development and implementation. The directive also established the National Plan Coordination staff, which became the Critical Infrastructure Assurance Office, an interagency office that is housed in the Department of Commerce and is responsible for planning infrastructure protection efforts. In addition, the directive designated "lead agencies" to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electric power industry. Similarly, regarding special function areas, the Department of Defense (DOD) is responsible for national defense, and the Department of State is responsible for foreign affairs. To facilitate private-sector participation, PDD 63 encouraged creation of Information Sharing and Analysis Centers (ISAC) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the NIPC. Figure 2 depicts the entities with critical infrastructure protection responsibilities as outlined by PDD 63.

Figure 2: Critical Infrastructure Protection Responsibilities, as Outlined by PDD 63



The NIPC Is Assigned A Broad Set Of Responsibilities

The NIPC was originally established by the Attorney General in February 1998 as an outgrowth of the FBI's Computer Investigations and Infrastructure Threat Assessment Center, which is a joint criminal and intelligence operation focused on computer crimes and threats to the national information infrastructure. According to the Attorney General, the NIPC was to become the government's lead mechanism for responding to infrastructure attacks.

In May 1998, PDD 63 authorized the FBI to expand the NIPC and directed the NIPC to gather information on threats and coordinate the federal government's response to incidents affecting infrastructures. According to the NIPC legal counsel, the NIPC was placed in the FBI because of the bureau's broad legal authority to collect, retain, and share information about potential cyber threats to the nation's critical infrastructures. In addition, the NIPC benefited from the FBI's jurisdictional authority and investigative capability, including conducting and coordinating criminal and foreign counterintelligence investigations within the United States. The directive further assigned the NIPC, operating under these authorities, specific responsibilities for

- issuing timely warnings on threats and attacks;
- providing comprehensive analyses on threats, vulnerabilities, and attacks;
- facilitating and coordinating the government's response to cyber incidents;
- providing law enforcement investigation and response;
- mitigating cyber attacks;
- monitoring reconstitution efforts; and
- promoting outreach and information sharing.

The following documents provide additional detail on the NIPC's mission and operational requirements:

- The FBI's *National Infrastructure Protection and Computer Intrusion Program Plan*, issued in April 1999 and updated in October 2000, outlines specific goals and strategies aimed primarily at developing a national investigative and response capability, especially as they relate to FBI field office activities.
- The unclassified version of the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan*, issued in September 1999, stresses the need for the NIPC to interact with other federal

counterterrorism and law enforcement efforts and provides specific details on NIPC programs, objectives, and requirements, such as analysis and warning operations, crisis management responsibilities, the Key Asset Initiative, and the InfraGard Program.
- The President's *National Plan for Information Systems Protection*, issued in January 2000, reiterates much of what was contained in the FBI's April 1999 program plan and the Attorney General's plan. However, it contained a broader description of governmentwide efforts and described how other federal entities might interact with the NIPC.

PDD 63 covered both physical and computer-based threats. However, the NIPC's efforts have pertained almost exclusively to computer-based threats, since this was an area that the leaders of the administration's critical infrastructure protection strategy viewed as needing attention. For example, the FBI 1998 Strategic Plan identified the protection of the national information infrastructure as one of the Bureau's highest priorities. The President's issuance of the *National Plan* further illustrated the administration's interest in this area. In addition, other components of the FBI had a lead role in addressing physical threats. Specifically, the Attorney General's 1999 plan noted that in the event of physical attacks on key infrastructures, the investigative response would be handled by FBI criminal investigative or counterterrorism components. In such cases, the NIPC would serve in a supporting role, providing relevant information about the victim infrastructure and other focused analytical or intelligence products.

Currently, the NIPC is located in the FBI's Counterterrorism Division, which is 1 of 11 FBI headquarters divisions headed by assistant directors who report to the FBI Director. The NIPC Director reports directly to the Assistant Director for Counterterrorism.

The NIPC is organized into three sections reflecting the mission areas identified by PDD 63.

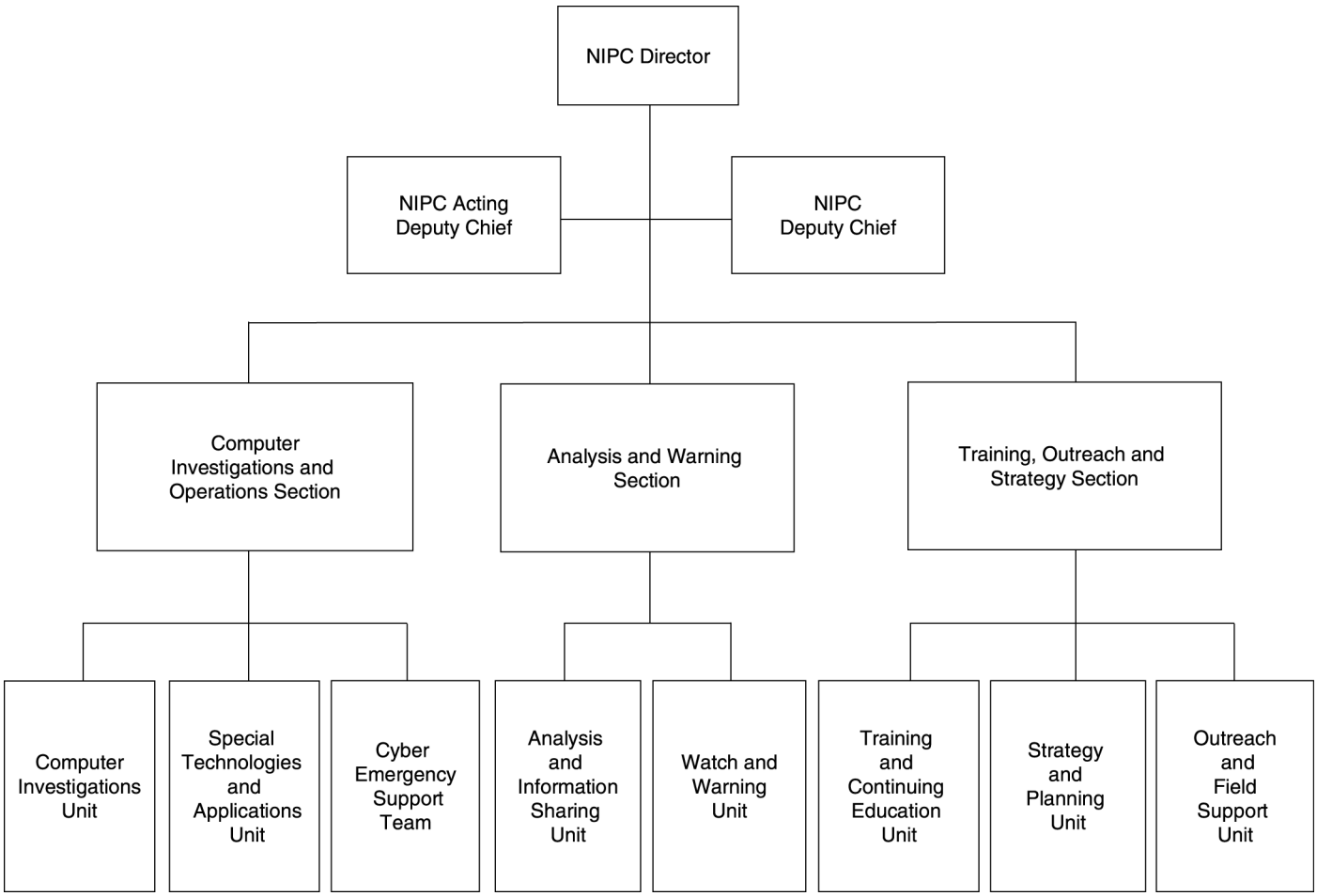
- The Computer Investigations and Operations Section is to support and, where necessary, coordinate computer investigations conducted by the FBI's 56 field offices and approximately 400 sublocations throughout the country; provide expert technical assistance to investigations; and coordinate the response to a national-level cyber incident.
- The Analysis and Warning Section is to provide tactical analytical support during a cyber incident and develop strategic analyses of

threats for dissemination to both government and private-sector entities so that they can take appropriate steps to protect themselves.

- The Training, Outreach, and Strategy Section is to coordinate the training of investigators in the FBI field offices, other federal agencies, and state and local law enforcement regarding computer-based threats. It also is to coordinate outreach activities with private industry and government agencies to build the partnerships that are key to the NIPC's investigative and warning missions. In addition, this section manages efforts to catalog information about individual "key infrastructure assets" and manages the InfraGard Program, which provides a forum for private industry and the NIPC to share information.

Figure 3 shows the NIPC's organization and identifies subunits in each of its three major functional sections.

Figure 3: NIPC Organizational Chart



Source: NIPC.

Objectives, Scope, and Methodology

Our objectives were to evaluate the progress that the NIPC has made in

- developing national capabilities regarding cyber threats for analyzing threat and vulnerability data and issuing warnings;
- enhancing its capabilities for responding to cyber attacks; and
- outreach and sharing information with government and private-sector entities, including the progress made regarding the InfraGard Program and development of the key asset database.

In addition, we were asked to determine the purposes for which the NIPC used funding provided for fiscal years 1999 and 2000.

To determine the NIPC's progress in developing capabilities for issuing warnings and analyzing threat and vulnerability data, we reviewed analytical reports that the NIPC had issued and held discussions with officials from the NIPC's Analysis and Warning Section. We observed a demonstration of the NIPC's watch and warning procedures and reviewed pertinent policies, guidance, and plans. To gain a more thorough understanding of the challenges associated with analyzing and reporting computer-based incidents and determine how the NIPC's responsibilities relate to those of other federal agencies, we met with officials in the intelligence community and in DOD who were involved in threat analysis and warning activities.

To determine the NIPC's progress in enhancing its capabilities for responding to cyber attacks, we reviewed pertinent policies, guidance, plans, and other supporting documentation and interviewed officials in the NIPC's Computer Investigations and Operations Section and Analysis and Warning Section. We visited 4 of the FBI's 56 field offices, which we selected because they were performing a diverse set of NIPC-related activities. Three of these field offices—in New Orleans, San Francisco, and Washington, D.C.—had full NIPC squads. The fourth field office, in Pittsburgh, had a NIPC team and the only interagency task force for investigating computer intrusions. During these visits, we observed operations related to investigating and responding to computer-based incidents and met with FBI agents involved in these activities.

To determine the NIPC's progress in outreach and information sharing with government and private-sector entities, we interviewed officials from the NIPC's Training, Outreach, and Strategy Section and from the three Information Sharing and Analysis Centers (ISAC) that had been established at the time of our review. (A fourth ISAC for the information technology industry, announced in January 2001, was not covered by our review.) These centers pertained to the financial services industry, the telecommunications industry, and the electric power industry. In addition, we observed a meeting sponsored by the FBI's Washington, D.C., field office to promote participation in the NIPC's InfraGard information-sharing program, and a training session on collaborative efforts by the North American Electric Reliability Council and the NIPC. We also discussed the InfraGard Program and efforts to develop a database of key infrastructure assets with responsible officials at the NIPC and four FBI field offices.

Further, we reviewed a variety of documents related to these outreach and information-sharing efforts.

To gain a more thorough understanding of the adequacy of the NIPC's progress regarding our first three objectives, we reviewed various documents that describe the NIPC's responsibilities. These included the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan* and *The National Plan for Information Systems Protection*, issued by the President in January 2000. We also met with federal officials outside of the FBI who were involved with federal critical infrastructure protection efforts. These included the National Coordinator and officials from the Office of Management and Budget (OMB) , the intelligence community, DOD, the Critical Infrastructure Assurance Office, a former Commissioner from the President's Commission on Critical Infrastructure Protection, current and former detailees to the NIPC from other organizations, and key persons involved in the creation of PDD 63. In addition, we interviewed the NIPC's Director, deputy director, and principal legal counsel.

To determine the purposes for which the NIPC used funding provided for fiscal years 1999 and 2000, we reviewed pertinent congressional reports, plans, guidance, and budget documents and reports on obligations developed for us by FBI and NIPC officials. We also held discussions with FBI finance division officials and NIPC headquarters officials responsible for funding-related decisions and for accounting for those funds. We reviewed the provided information for consistency; however, we did not independently verify the data on obligations or review the NIPC's related internal-control procedures.

We performed our audit work from May 2000 through February 2001 in accordance with generally accepted government auditing standards. We received comments on a draft of this report from the Director of the NIPC and the Special Assistant to the President and Senior Director for Legislative Affairs. The comments are printed in full in appendixes I and II, respectively.

Multiple Factors Limit Progress in Developing National Analysis and Warning Capabilities

The NIPC's progress in developing national capabilities for analyzing vulnerability and threat data and issuing timely warnings of computer-based attacks, as described in PDD 63, has been limited. However, the NIPC has laid a foundation for further governmentwide efforts in these areas. Analysis and warning capabilities are needed to improve the government's ability to recognize changes in threat conditions, detect impending attacks, or effectively warn government and industry of such attacks in time to prevent serious damage.

Since it was established in 1998, the NIPC has issued a variety of analytical products. Most of these products have been based on the work of others, with some original NIPC analysis. The majority of the NIPC's original analysis has been tactical analysis performed in support of investigations of individual incidents. Progress in developing strategic analysis to assess the broader, long-term implications of such threats has been impeded because there is no generally accepted methodology for threat analysis, adequate staff and expertise have not been supplied, and data on infrastructure vulnerabilities have not been provided by industry sectors. Overcoming these obstacles will require significant interagency efforts and resources.

The NIPC has developed rudimentary capabilities for issuing warnings. From February 1998 through December 2000, it issued 81 alerts, advisories, and assessments. However, most of these warnings pertained to attacks already underway and, therefore, may have been too late for recipients to take mitigating action. The NIPC's efforts to develop a more robust warning capability have been impeded by a lack of staff expertise and because a governmentwide or nationwide framework for promptly collecting and analyzing incident information has not been established. In addition, issuance of timely warnings has been hindered by the need to protect sensitive information and verify the accuracy and significance of reported incidents before issuing related warnings.

Further, two fundamental problems make it difficult to measure the NIPC's progress and determine its needs for developing more substantive analysis and warning capabilities. First, the NIPC's roles and responsibilities have not been fully defined and are not consistently interpreted by other federal agencies responsible for critical infrastructure protection, and these entities have not provided the NIPC the support envisioned by PDD 63. Second, the NIPC has not developed a comprehensive and integrated, multiyear plan of action to prioritize and guide its analysis and warning efforts and to identify needed resources.

NIPC officials are aware of these problems and have taken some steps to address them. However, many of these problems cannot be resolved by the NIPC alone and will require governmentwide efforts. At the close of our review, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism said that options for adjusting the federal strategy for critical infrastructure protection were being considered, including a reassessment of roles and responsibilities pertaining to the development of analysis and warning capabilities.

PDD 63 Directs the NIPC to Develop Analysis and Warning Capabilities

The analysis and warning capabilities called for by PDD 63 presume that analytical processes can be developed to detect precursors to computer-based attacks so that advance warnings can be issued and protective measures implemented. Since the 1990s, the national security community and the Congress have identified a need to establish analytical and warning capabilities, which are sometimes referred to as "indications and warnings," to protect against strategic computer attacks against the nation's critical computer-dependent infrastructures. Such capabilities involve (1) gathering and analyzing information for the purpose of detecting and reporting hostile or otherwise potentially damaging actions or intentions and (2) implementing a process for warning policymakers and allowing them time to determine the magnitude of the related risks.

PDD 63 specifically assigns the NIPC the responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities and timely warnings of actual or potential attacks. According to the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan*, issued in 1999, the NIPC's functions are to include analyzing risks to infrastructures, understanding the indicators of a computer-based attack, establishing the technical capability to identify indicators, and determining what constitutes an attack by a foreign power. The January 2000 *National Plan for Information Systems Protection* further specifies that the NIPC will combine the information it obtains on computer-based attacks with intelligence, law enforcement, and other indicator information to identify patterns that may signal that an attack is underway or imminent.

Analyses Have Primarily Supported Investigations of Individual Incidents

To develop the analytical capabilities specified in PDD 63 and related requirements, the NIPC created the Analysis and Information Sharing Unit (AISU) in May 1998. According to the *National Infrastructure Protection and Computer Intrusion Program Plan*, the AISU is to provide both (1) tactical analytical support during a cyber incident and (2) strategic analyses of threats. Tactical support involves providing current information on specific factors associated with incidents under investigation or specific identified vulnerabilities. Examples of tactical support include analysis of (1) a computer virus delivery mechanism to issue immediate guidance on ways to prevent or mitigate damage related to an imminent threat or (2) a specific computer intrusion or set of intrusions to determine the perpetrator, motive, and method of attack.

In contrast, strategic analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. For example, strategic analyses may identify long-term vulnerability and threat trends that provide advance warnings of increased risk, such as emerging attack methods. Strategic analyses are intended to provide policymakers with information that they can use to anticipate and prepare for attacks, thereby diminishing such attacks' damage.

Analyses Have Primarily Addressed Tactical Issues

Since its establishment, most of the AISU's activities have been focused on tactical analyses related to investigations of individual cyber incidents or notices of recently reported vulnerabilities. As of early November 2000, the AISU had produced 15 tactical situation reports related to law enforcement investigations. Twelve of these situation reports were associated with investigations of denial-of-service attacks that affected numerous Internet entities, including E-Bay and Yahoo, in February 2000. In addition to efforts resulting in written products, the AISU has assisted in investigations of other incidents that were quickly resolved and did not result in formal reports. For example, in July 2000, AISU analysts spent several days supporting efforts to monitor an incident associated with a classified system that did not evolve into a significant incident and, therefore, did not result in a written report.

In addition, since 1998, the AISU has provided analytical support related to a counterintelligence investigation, which involves a complicated series of computer intrusions into federal agencies, universities, and private-sector systems. As of December 2000, this effort had resulted in 12 analytical

documents, which, unlike most of the AISU's other efforts, included both tactical and strategic analyses. NIPC officials say that these analyses have provided valuable experience that the AISU is using to develop improved methods for identifying perpetrators and understanding their actions. For example, the NIPC initiated Project La Resistance, which is a strategic effort to analyze information gathered from disparate sources, including law enforcement and intelligence agencies, private industry, and other open sources, to identify linkages and commonalties among incidents and perpetrators.

The AISU has also issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis. Its most widely disseminated documents include a biweekly publication called *CyberNotes*, a compilation of reports by other sources on software vulnerabilities, hacker techniques, and virus information, which is intended for use by security professionals. *CyberNotes* is presented in a summary table format that includes pertinent information on each vulnerability, such as vendor and operating system, software name, potential impact, remedies, and an indication of whether any attacks have actually exploited the vulnerability or attack technique. The NIPC also produces and broadly distributes the *Daily Watch,* a listing of daily developments affecting infrastructures, which is compiled from a range of sources. In January 2001, the NIPC introduced *Highlights* (formerly known as *Critical Infrastructure Developments*) as a publication intended to provide information on infrastructure protection issues, with a specific emphasis on computer and network security matters.

Limited Strategic Analysis Performed

While the NIPC has provided support to the previously mentioned counterintelligence investigation and input into two intelligence community documents, including the recent National Intelligence Estimate on cyber threats, overall, it has performed limited strategic analysis. As a result, information on individual incidents or groups of incidents has not been fully taken advantage of to assist in identifying broader, longer-term risks. For example, in October 1999, the NIPC issued an advisory on a Trojan-horse program dubbed "RingZero," describing it as an "aggressive reconnaissance technique" used to obtain detailed information on systems that could be used to facilitate future attacks.[1] The NIPC advisory was

[1]NIPC Advisory 99-024: RingZero Trojan Program Issued at 3:00 p.m., EDT, October 22, 1999.

based on analyses obtained from the Systems Administration, Networking, and Security (SANS) Institute, which is a cooperative research and education organization, and the Naval Surface Warfare Center. These analyses highlighted the possible malicious uses of RingZero for anonymously performing large distributed attacks. However, the NIPC made no attempt to determine the potential strategic implications of RingZero and more thoroughly understand the related risks to national infrastructures. Additional analysis was not performed because, according to the Chief of the AISU, staff were diverted to other incidents of more immediate concern.

NIPC officials told us that the RingZero analysis was an example of how their efforts to develop strategic analysis capabilities had been limited because the AISU's analysts were fully engaged in supporting a growing stream of new and ongoing investigations of computer-based incidents. This point was corroborated in an October 2000 *National Infrastructure Protection and Computer Intrusion Program Plan*, issued by the FBI's Counterterrorism Division, which stated that, while over 1,000 computer crime investigations were underway, the NIPC could only provide regular analytical support to fewer than a dozen of the most important cases.

Impediments to Developing More Substantive Analytical Capabilities

The experts we interviewed at the NIPC and other federal agencies agreed that developing substantive capabilities for analyzing computer-based threats is a formidable task, especially in the area of strategic analysis. No generally accepted methodology in this area exists, and analytical expertise and reliable data on infrastructure vulnerabilities are in short supply. These factors have impeded the NIPC's progress in this area.

Lack of Methodology for Strategic Analysis

According to federal intelligence and national security officials, no generally accepted methodology for strategic analysis of cyber threats to the nation's infrastructures has been developed. Lacking are a standard terminology, a standard set of factors to consider, and established thresholds for determining the sophistication of attack techniques. As a result, no proven or generally accepted approach exists that the NIPC can readily adopt to perform such analyses. The intelligence community officials we met with said that developing such a methodology would require an intense interagency effort and a dedication of significant resources.

Lack of Needed Staff and Expertise

According to senior NIPC officials, the AISU has depended to a large extent on detailees from other agencies to supplement FBI staff. Although the FBI has investigative capabilities, it acknowledges that it lacks staff who are experienced in critical infrastructure operations and intelligence analysis. The NIPC Director told us that the use of detailees was intended to be a means of rapidly assembling an analytical capability from existing expertise within the federal government and that, in his view, it was important for the NIPC to draw on the expertise and diverse perspectives of personnel from other agencies. Accordingly, the chief of the Analysis and Warning Section, which includes the AISU, and the AISU chief, at the time of our review, were detailees from the intelligence community.

NIPC officials also attribute the limited progress of the Analysis and Warning Section and the AISU to sustained leadership vacancies. According to NIPC records, the Chief of the Analysis and Warning Section position, which was to be filled by the Central Intelligence Agency (CIA), was vacant for about half of the NIPC's 3-year existence. Similarly, NIPC records show that a National Security Agency detailee position was vacant for approximately 17 months between May 1998 and April 2000. As a result, the NIPC could not fully benefit from the experience of these intelligence community officials in developing the required capabilities.

In addition, fewer detailees have been provided for other AISU positions than were originally anticipated, and most positions have been filled with FBI analysts. Since its creation in 1998 through the end of fiscal year 2000, the AISU has operated with an average of about 13 analysts. Ten of these positions have been held by FBI analysts, and three positions have been held, sometimes on an intermittent basis, by detailees from other federal agencies or from international partners, such as Canada and the United Kingdom. An additional three detailee positions were designated by the NIPC but were not staffed by the other involved federal agencies. In August 2000, the Analysis and Warning Chief estimated that the AISU needed about 24 analysts to provide a foundation for building adequate analytical capabilities. This would allow the NIPC to devote about three analysts to each of the eight industry sectors identified in PDD 63.

Through interviews with NIPC officials and individuals from other federal agencies who had been detailed to or otherwise associated with the NIPC, we identified two factors that contributed to agencies' not providing the number of experienced detailees originally anticipated. First, federal employees with experience in computer security and information technology management are in short supply, and agencies need those

available to support their own operations. As a result, agencies are reluctant to provide such valued staff to the NIPC. Second, of the 25 individuals we interviewed who had been detailed to the NIPC, 16 expressed negative comments about their work experience there. In particular, the detailees noted that FBI procedures prevented them from being involved in decisionmaking and limited their access to information. Some of the detailees felt that they were not provided the same level of respect and support as were the FBI agents who were assigned to the NIPC. For example, one detailee assigned to the NIPC for almost 18 months during 1999 to 2000, observed that detailees had different badges, could not access some computer systems, and could not sign procurement orders. However, by the summer of 2000, the situation had improved; detailees were given badges similar to FBI personnel, increased access to computer systems, and authority to sign some procurement forms.

Although NIPC officials cited a need for more personnel, they also cited a need for personnel with more experience and expertise in computers, infrastructure operations, and intelligence analysis. NIPC officials said that most of the FBI employees assigned to the AISU have had limited expertise in these areas and have lacked the skills necessary to perform the assigned functions. The FBI's 1998–2003 Strategic Plan corroborated these assertions, noting that FBI analysts often have had little or no training in intelligence analysis and lack experience in the subject matter for which they are responsible. According to one NIPC manager, additional expertise could be obtained by hiring analysts from outside of the FBI. However, NIPC officials say they have been precluded from doing so because the NIPC must stay within the authorized FBI staffing levels. NIPC officials said that this shortage of expertise and skills has especially limited the NIPC's ability to establish a viable strategic analysis capability, since this requires sustained efforts over a period of time. FBI and NIPC officials are aware of this problem and, in 1998 and 2000, the Attorney General and the FBI director wrote to agency heads requesting detailees. Also, in November 2000, the FBI Director sent a letter to the Assistant to the President for National Security Affairs stating that "without additional support from other federal agencies, our ability to effectively detect, warn of, and respond to cyber attacks will not be adequate to address the ever growing threat." In addition, NIPC officials told us they were developing a plan and budget justification that detailed the need for an increase in NIPC staff.

Inadequate Data on Infrastructure Vulnerabilities

The AISU's strategic analysis capabilities depend to a large extent on the availability of technical infrastructure assessments that provide industry-specific data on factors such as critical system components, known

vulnerabilities, and interdependencies. Under PDD 63, eight infrastructure segments were to be assessed by each industry sector's lead agency and industry representatives. For example, the Department of Transportation was directed to work with the transportation industry, and Commerce was to work with the telecommunications sector to develop their respective sector technical assessments.

According to the *National Plan*, the NIPC was to use these assessments in combination with foreign intelligence information, information from law enforcement investigations and operations, and voluntary private-sector reports, to develop comprehensive strategic assessments of risk. According to the Attorney General's plan, such comprehensive assessments are important because they are to form the basis for identifying indicators of potentially malicious or damaging activity and developing related intelligence collection requirements. In addition, these assessments provide input for a variety of NIPC products, including alerts and advisories.

Most of the industry assessments have not, however, been performed, and none have been provided to the NIPC. NIPC officials told us that assessments had been at least partially performed for the electric power, transportation, and water sectors. However, they had received no detailed written assessments and, as a result, could not benefit from their findings. In addition, in 2000, NIPC initiated assessments of telecommunications and electric power. According to NIPC officials, these assessments were intended to develop relevant products for the industry sectors and encourage sectors to participate more in PDD 63. At the close of our review, these documents remained in draft form.

The NIPC Has Developed a Rudimentary Warning Capability

To provide a warning capability as required by PDD 63, the NIPC established the Watch and Warning Unit. The unit's objective is to identify attacks that appear imminent and alert government entities, businesses, and the public, so that significant damage can be averted. While some warnings have been issued in time to avert damage, most of the warnings, especially those related to viruses, have pertained to attacks that were already underway.

Several factors, some of which are beyond the NIPC's control, have hindered the NIPC's ability to provide advance warnings. Specifically, no comprehensive governmentwide or nationwide data-collection and analysis framework has been established to provide the NIPC with

information on unusual or suspicious computer-based activity before the occurrence of actual incidents. In addition, the Watch and Warning Unit's ability to issue warnings is slowed by a shortage of experienced watch officers and the need to verify the accuracy of the input it receives and ensure that sensitive information is protected.

Number of Warnings Has Increased, but Value in Protecting Systems Is Largely Unknown

Since its establishment in 1998, the NIPC has issued 81 warnings that were based on the work of its Watch and Warning Unit. Many of these alerts were posted on the Internet and were available to the public. Other alerts were targeted to specific industries or individual organizations that the NIPC deemed to be at special risk.

The NIPC categorizes its warnings as follows. The most serious is an "alert," which provides information on a major threat or on imminent or in-progress attacks targeting specific national networks or critical infrastructures. The second most serious type of warning is an "advisory," which provides information on significant threats or incidents and suggests that organizations strengthen their readiness posture. The third and least serious type of warning is an "assessment," which provides broad, general incident or issue awareness information that is both significant and current but does not necessarily suggest immediate action. Before March 2000, the NIPC issued notifications referred to as "warnings," which were similar to what it now refers to as alerts. The NIPC deleted this category and added the assessment category so that its warning system would more closely be aligned with the FBI's system for warnings about terrorist acts. In some cases, multiple warnings are issued that pertain to only one type of attack or incident. For example, in May, June, and August 2000, the NIPC issued nine alerts on the ILOVEYOU virus and related variations. The number and type of warnings issued by the NIPC in 1998 (February - December), 1999, and 2000 are summarized in table 1.

Table 1: Warnings Issued by the NIPC, 1998, 1999 and 2000

Type of warning	Number of warnings			
	1998 (Feb. - Dec.)	1999	2000	Total
Alert	5	7	11	23
Advisory	1	18	14	33
Assessment[a]	N/A	N/A	11	11
Warning[a]	4	10	N/A	14
Total	**10**	**35**	**36**	**81**

N/A = not applicable

[a]Before March 2000, the NIPC issued notifications referred to as "warnings," which were similar to what it now refers to as "alerts." The NIPC deleted this category and added the assessment category so that its warning system would more closely be aligned with the FBI's system for warnings about terrorist acts.

Source: GAO analysis of NIPC data.

Most of the NIPC's warnings illustrated in table 1 pertained to attacks underway; few preceded an imminent attack. One senior NIPC official noted that the NIPC currently lacks the information and the necessary understanding to identify discrete indicators that might be precursors to a computer-based attack. As a result, most of its warnings are based on reports of attacks in progress. However, in late 1999 and 2000, there were several instances when the NIPC was able to provide warnings before an attack was actually launched. These included the following examples:

- In April 2000, the NIPC obtained information from a law enforcement investigation that 478 serious (root-level) compromises had been perpetrated globally in an effort to create a distributed denial-of-service attack. The NIPC coordinated efforts to warn victims, individually, by working with 11 FBI legal attachés located abroad and through the FBI field offices in the United States. According to the NIPC, many victims had been unaware of their systems' compromise before the warning.
- In December 1999, multiple reports of the presence of distributed denial-of-service tools on computer systems in the United States prompted the NIPC to issue an alert, its most urgent warning. According to the NIPC, these tools were capable of generating sufficient network traffic to congest targeted networks or systems, thus rendering them inoperable. The NIPC supplemented its alert with a software program that system administrators could use to detect the presence of denial-of-service attack tools on their systems.

While the NIPC has issued warnings directly to hundreds of individuals and entities, and made many of its alerts, advisories, and assessments publicly available through its Web site, it does not have any reliable information on the effectiveness of these warnings. For example, NIPC does not develop statistics on the number of visitors to its Web site or routinely solicit feedback on the effectiveness of its warnings from industry or the public. NIPC officials told us that they informally solicit feedback and had received a great deal of unsolicited feedback on NIPC products. They said that further efforts in this area were constrained by limited resources. Also, they noted that a challenge inherent in providing warnings is that there is no way to ensure that potential victims will hear or heed the warning.

Watch and Warning Procedures Formalized During 2000

During the last half of 2000, the Watch and Warning Unit formalized standard operating procedures to guide the activities of watch officers. Before this, informal procedures had evolved as the unit gained experience, but many had not been fully documented. In addition, many watch officers were detailees from other agencies, and turnover of staff had been rapid, making the need for standard, documented procedures especially important.

The new procedures are intended to ensure that watch officers perform their duties completely and consistently and establish standard criteria and procedures for issuing warnings. As such, they describe watch officer responsibilities and provide a detailed list of activities to be conducted at specified intervals. The procedures also describe a carefully ordered process for assessing an incident; convening a watch advisory committee; developing alerts, advisories, and assessments; and disseminating warnings.

Barriers to Issuing Early Warnings

Even when the NIPC becomes aware of an imminent threat, four factors hinder its ability to issue early warnings: (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks; (2) a shortage of skilled staff; (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents; and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

No Comprehensive Data-Collection and Analysis Framework

Unlike watch and warning efforts for attacks from nuclear and conventional weapons, which are supported by an array of satellites and other data-collection and analysis mechanisms, no comprehensive governmentwide or nationwide data-collection and analysis framework has been established for (1) developing information on what constitutes unusual or suspicious activity associated with computers supporting critical operations, (2) recognizing such activity, and (3) promptly reporting the activity to the NIPC or others for further analysis to determine if a warning is appropriate. As a result, the Watch and Warning Unit develops its warnings on the basis of analyses developed by the AISU, which it supplements with information gathered from the Internet and from telephone calls and e-mails from government and industry sources.

Officials involved in developing indications and warnings at DOD told us that establishing more comprehensive and effective mechanisms for detecting computer-based attacks are likely to take significant effort. According to the 1996 *Report of the Defense Science Board Task Force on Information Warfare Defense*, it took the United States over four decades to identify the indicators for nuclear and conventional attacks and optimize the collection and reporting systems to perform analysis needed for watch and warning. Defense officials told us that developing reliable indications of impending computer-based attacks would be even more difficult because attacks can be launched by small, loosely aligned groups. Such planned attacks are difficult to identify because the perpetrators do not always have the bureaucratic organization or command and control structure that allows their doctrine, organization, and capability to be observed in advance of an attack. In addition, the ability of such groups to quickly develop networks and maintain anonymity makes it very difficult to create the types of predictive methodologies that have evolved for monitoring traditional, noncyber threats.

Several federal efforts are planned or underway to develop warning indicators and mechanisms for promptly communicating alert data. For example, the NIPC and the electric power industry have developed a voluntary set of reporting requirements and thresholds for voluntary information sharing and data analysis. This "Indications, Analysis and Warning" program, piloted in 1999, is intended to (1) establish computer connectivity with electric power industry components, (2) develop agreed-upon criteria for attack indicators, and (3) implement criteria for information sharing with the NIPC. (Chapter 4 of this report discusses in greater detail the NIPC's efforts to establish cooperative, information-sharing relationships with government and private-sector sources.) In

addition, the National Security Agency's National Security Incident Response Center, which acts as a focal point for addressing computer incidents affecting national security information systems, maintains a database on computer incidents and their sources. In 1998, the response center recorded more than 5,700 computer incidents, which originated from foreign and domestic sources. However, no such data-collection framework is being developed on a governmentwide or national basis.

Shortage of Skilled Staff

NIPC has difficulty staffing its 24-hour watch operations with skilled staff. During 1999 and 2000, the Watch and Warning Unit had an average of 12 employees, who monitored the Internet and other media to identify reports on computer-based attacks. Initially, the unit operated 5 days a week, 16 hours a day. In December 1999, the NIPC initiated continuous watch operations—24 hours a day, 7 days a week. The NIPC's goal is to have four people on each 12-hour shift. NIPC officials said that they have not met this goal because they have not had enough staff who possess an understanding of the Internet and the implications of computer attack techniques to recognize potentially serious incidents. Officials told us that, as a result, some shifts could not be adequately staffed.

Avoiding Undue Alarm

While the NIPC considers all types of incidents and attacks, it is important that the NIPC limit its public warnings to those that appear to present significant risk. Computer-based attacks and other potentially destructive incidents are becoming more common, but, according to NIPC officials, most incidents result in little or no significant damage. For example, officials assert that approximately 20 to 30 new computer viruses are disseminated daily, with over 50,000 known viruses being in existence. From their experience, NIPC officials determined that most of these viruses did not warrant a public warning because they were not very damaging, did not propagate easily, or were readily detected by existing antivirus software.

Issuing too many warnings on incidents that ultimately do little or no harm would diminish the NIPC's credibility, and computer users might begin to ignore important warnings. In May 2000, the NIPC Director stated that "creating an unnecessary panic or perpetuating a virus hoax could be just as damaging as a real virus if it caused people to unnecessarily disconnect from the Internet or shut down e-mail."[2] Accordingly, the NIPC takes time

[2]Statement for the Record of Michael A. Vatis, NIPC Director, before the Senate Committee on Judiciary, May 25, 2000.

to ensure that the reports it obtains are credible and to determine if incidents, attacks, and viruses are significant enough, in terms of their potentially destructive impact, to warrant a public warning. The procedures defined by the NIPC in August 2000 state that analyzing a potential threat, determining the need for a warning, and disseminating the warning can take several hours and involve a wide range of contacts with NIPC personnel and outside entities, including computer incident response centers and software manufacturers.

The NIPC's ability to perform such analyses in a timely manner is closely linked to the extent of technical and analytical expertise that it has available on a 24-hour basis. Shortfalls in such expertise have limited the NIPC's ability to promptly determine which incidents merit issuance of an immediate warning.

Protecting Sensitive Information

In many cases, the NIPC learns of a computer-based threat from intelligence sources or as part of a criminal investigation. In these cases, the NIPC takes special precautions to ensure that warnings do not inappropriately disclose sensitive information, thus balancing the need to protect evidentiary data with the need to issue timely warnings.

Such precautions can be tedious and time-consuming. Before disseminating national security or intelligence information, the NIPC works with the originating agency to delete sensitive information, which is a process often referred to as sanitizing the information. For example, to release information from a classified source, such as an intelligence report, the NIPC obtains permission from the analyst who wrote the report. Then, according to NIPC officials, they must submit a draft of the sanitized version to the originating intelligence analyst for review and release. This process can involve several exchanges of drafts, thereby slowing the warning process.

Sanitizing law enforcement information can also cause delay. According to NIPC officials, while there is a common understanding about procedures for handling classified information and the punishments for mishandling it, there is no legal framework detailing how law enforcement sensitive information is to be handled. As a result, many in the law enforcement community are hesitant to share information with officials in the defense and intelligence communities or with the private sector. Another deterrent is that law enforcement sensitive information, such as classified intelligence information, may impact undercover operations, and

mishandling it may seriously harm operations and place sources of information at risk.

Several officials we met with outside of the NIPC noted the difficulty inherent in balancing the benefits of warning the public with the benefits of protecting information needed to apprehend a perpetrator and prosecute a criminal case. Investigations may yield unique information that, when translated into warnings, can both prevent damage as well as help identify additional victims of a related attack. NIPC officials agreed and said that, during 1999 and 2000, they have attempted to make warning a priority by encouraging investigators and analysts to disseminate warnings that protect law enforcement, while still providing industry and government information needed to mitigate damage from computer-based attacks. According to NIPC records, on 18 occasions from March 1999 through October 2000, the NIPC issued warnings that were based on information from ongoing criminal and foreign counterintelligence investigations.

However, in February 2001, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism told us that issues still remained to be resolved to facilitate the sharing of such information. For example, he asserted that, in some instances, it would be helpful if the NIPC shared more information during the initial phase of an investigation so that other federal entities can take appropriate action to protect their operations.

Other Factors Impeding Development of Analysis and Warning Capabilities

In addition to the impediments discussed, two significant factors make it difficult to evaluate the NIPC's progress in developing analysis and warning capabilities and may impact the viability of the government's broader strategy for protecting the nation's critical infrastructures from computer-based attacks. The first factor is that the NIPC's roles and responsibilities have not been fully defined and are not consistently interpreted by other entities responsible for critical infrastructure protection. The second factor is that the NIPC has not developed a comprehensive, integrated plan that describes its goals for developing analysis and warning capabilities and the actions and related resources needed to achieve them.

Details of NIPC Roles and Priorities Inadequately Defined and Communicated

The government's strategy and subordinate plans for protecting the nation's critical infrastructures from computer-based attacks, including the NIPC's role, have not been clearly articulated. While PDD 63 established December 2000 as the deadline for achieving an initial operating capability

and May 2003 for achieving full operational capability of key functions, such as warning capability, neither the directive nor the subsequent *National Plan for Information Systems Protection* defined what such capabilities would include. PDD 63 describes general goals and provides an outline of the responsibilities assigned to the NIPC, but the directive provides few details regarding the NIPC role and its relationship to other entities, especially those involved in analysis and warning for national security. The *National Plan* provided little additional information pertaining to the NIPC, noting that the plan "will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats."

Interpretation of NIPC's Role Is Not Consistent

In a September 1998 report, shortly after the initial issuance of PDD 63, we noted the importance of developing a governmentwide strategy that clearly defines and coordinates the roles of new and existing federal entities to ensure governmentwide cooperation and support for PDD 63.[3] At that time, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the Assistant to the President for National Security Affairs ensure such coordination. In written comments on that report and at a November 1998 meeting, senior officials involved in implementing PDD 63 told us that plans for such coordination were being implemented. However, our more recent meetings with representatives of the entities involved in the government's critical infrastructure protection showed that they do not share a consistent interpretation of the NIPC's roles and responsibilities in these efforts.

PDD 63 outlines a central national role for the NIPC. Specifically, it says the following:

> "The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts."

However, our discussions with officials in the defense, intelligence, and civilian agencies involved in critical infrastructure protection, and with OMB and the National Security Council showed that their views of the NIPC's roles and responsibilities differ from one another and, in some cases, from those outlined in PDD 63. Several expressed an opinion that

[3] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

this lack of consensus has hindered the NIPC's progress and diminished support from other federal agencies. Examples of their comments follow:

- The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who is responsible for implementation of PDD 63, told us that there is a conflict between the NIPC's responsibilities to (1) broadly gather, analyze, and share information on computer-based threats and (2) support the FBI's investigative activities, which usually preclude sharing of information associated with cases under investigation. He said that this conflict has impeded the NIPC's ability to fulfill its analytical and warning responsibilities and diminished the level of support it has received from other agencies and the private sector. He said that he believes the NIPC role should be limited to investigating incidents.
- OMB officials told us that they did not view the NIPC, as "the" national focal point for gathering information on threats, but as one of several centers devoted to providing information on threats to U.S. infrastructures. In addition, they said that the NIPC's focus was to be on law enforcement, as indicated by its placement within the FBI.
- Officials in the intelligence community said that they were uncertain what role the NIPC was supposed to play, and several noted that, for national security purposes, they viewed the NIPC as a second-tier participant that primarily received finished intelligence, rather than an organization that generated original, analytical products.
- Several officials involved in critical infrastructure protection efforts said that PDD 63 envisioned that the NIPC would combine the strength of agencies responsible for national defense, intelligence, and domestic law enforcement. However, fulfilling this vision sometimes conflicts with the FBI's primary mission of apprehending criminals and bringing them to justice. In particular, this conflict has led to questions about the NIPC's ability to lead response efforts should a widespread computer-based crisis occur.

NIPC officials maintain that PDD 63 and the *National Plan* clearly outline the functional responsibilities of the NIPC. Further, NIPC officials told us that, in their view, some agency officials say the NIPC's role is not defined properly either as an excuse for not providing support in the form of detailees or because the agencies believe that parts of the NIPC's mission should be performed elsewhere. The FBI Director corroborated this in a November 2000 letter to the Assistant to the President for National Security Affairs in which he stated "some agencies appear to question PDD 63 itself and would like to take parts of the NIPC's mission."

Lines of Authority Are Not Clear

It is unclear who has direct authority for the NIPC, who sets its priorities and procedures, and who provides oversight. PDD 63 states that the National Coordinator, who reports to the Assistant to the President for National Security Affairs, shall be responsible for coordinating the implementation of the directive. Accordingly, the National Coordinator contends that responsibility for NIPC oversight rests with him. However, because the NIPC is located within the FBI and the NIPC Director is subordinate to an FBI Assistant Director, the NIPC is also subject to FBI direction.

This situation may be impeding the NIPC's ability to carry out its mission. Examples include the following:

- The NIPC's budget requests—including staffing and other financial resources—are controlled by the FBI and the Department of Justice, raising concern among NIPC officials that the NIPC's priorities, which are intended to reflect the interests of national critical infrastructure protection, may be subordinated to the FBI's law enforcement priorities. NIPC officials told us that their repeated requests for additional resources as part of the budget process had not been approved by the FBI.
- Requests for detailees of agencies, such as the Departments of State, Energy, Defense, and the Treasury and the CIA, to support the NIPC have come from the FBI and Justice, rather than from the National Coordinator or the National Security Council, possibly raising questions regarding whether the NIPC's request for detailees had the full support of the Executive Office of the President.
- The NIPC proposal to create an operational advisory board comprising senior representatives from other agencies with key critical infrastructure protection roles and intended to resolve several issues—including the need for detailees and interagency expertise—was approved by the FBI Director but subsequently rejected by the National Coordinator, leaving the issues unaddressed.
- Existing agreements between the Executive Office of the President and Justice restricting disclosure of law enforcement information have inhibited the NIPC's ability to share information with the National Coordinator. For example, in a recent case, the NIPC Director was unable to share information about an investigation with the National Coordinator until officials in Justice had approved it.

The NIPC Has Not Been Integrated Into National Security Warning Procedures

The NIPC's role in providing warning has not been integrated into the national security warnings process, which provide a means of alerting the most senior federal officials, including the President, of serious or imminent threats to national security. Such warnings are developed and issued by the National Intelligence Council, which includes members from each federal intelligence agency. According to the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan*, the National Intelligence Council, the Joint Chiefs of Staff, the National Communications System, and the NIPC met in 1998 and 1999 to discuss how the NIPC should be integrated into the national warning system. The goal was to produce a warning system that met the requirements for national defense, law enforcement, and intelligence. However, no consensus was reached and no additional meetings were held. As a result, NIPC's role has not been formally recognized as part of the national security warning procedures.

Rules for Recognizing and Responding to a National Security Incident Have Not Been Established

The NIPC and the Defense and intelligence communities have not developed (1) criteria for determining when a computer-based attack should be treated as a national security event rather than as a crime and (2) protocols for placing the NIPC in a support role, rather than a lead role, should such a national security event occur. While computer-based attacks, to date, have not caused devastating damage and have not been treated as acts of war, NIPC and DOD officials agree that, under certain circumstances, such an attack could constitute an act of war or other immediate threat to national security.

PDD 63 recognized that, should an incident be deemed a threat to national security, responsibility for coordinating the response would fall to DOD or the intelligence community. Specifically, PDD 63 stated that, "depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community." Accordingly, NIPC officials said that there is a need to establish response protocols that will differentiate between national security concerns, criminal activity, and malicious mischief. DOD's Director for Information Assurance agreed, stating that, without such protocols, a national security crisis may not be recognized and addressed in a timely manner.

While some legal provisions and detailed protocols exist for placing the FBI in support of DOD for responses to terrorism, it is not yet certain whether the same provisions would apply to computer-based attacks. Such provisions and protocols are important because they provide, under certain circumstances, exemptions from prohibitions of the Posse Comitatus Act,[4] which bars DOD from participating in domestic law enforcement activities. A number of statutory exemptions permit DOD's involvement in dealing with domestic terrorist incidents. For example, if an exceptionally grave physical terrorist threat or incident exceeds FBI capabilities, a special operations task force may be established that places DOD in the lead and the FBI in a support role. According to Justice officials, these statutory exemptions often require a request from the Attorney General; concurrence by the Secretary of Defense; and, as a matter of policy, in most instances, approval by the President. To initiate this process, the President must issue an executive order and a proclamation—documents that are maintained in draft form so that they are ready for the President's signature, if needed.[5]

Senior NIPC officials told us that they intended that the operational advisory board that they had proposed establishing during 2000 would examine the existing protocols developed for physical terrorism and determine if they were sufficient in the event of a serious computer-based attack or if new protocols were needed. However, as previously mentioned, the National Coordinator turned down this proposal, and, as of December 2000, Defense and intelligence officials told us that there were no efforts underway to resolve this issue.

The NIPC Has Not Integrated Plans for Developing Analysis and Warning Capabilities

An additional factor impeding evaluation of its progress is that, as of December 31, 2000, the NIPC had not developed a comprehensive, integrated plan outlining its goals for developing analysis and warning capabilities and identifying needed resources. Instead, it has developed elements of a plan, which are contained in a variety of different documents. These include the following:

[4]The Posse Comitatus Act, Title 18 U.S.C. 1385.

[5] *Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy* (GAO/NSIAD-97-254, September 26, 1997).

- In 1999, the FBI outlined general goals and challenges related to developing analysis and warning capabilities in the *National Infrastructure Protection and Computer Intrusion Program Plan.* This plan recognized the need to (1) institutionalize a process for receiving real-time information relative to threats, incidents, and vulnerabilities pertaining to critical infrastructures and (2) develop analytical and communications skills and expertise in computer technologies. An updated version of the plan was issued in October 2000. However, both the 1999 plan and the 2000 update focus primarily on investigative capabilities being developed in FBI field offices.
- In 1999, the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan* provided detailed information on the intended operations of the NIPC, including analysis and warning as well as the identification of indicators. It also recognized that the development of NIPC capabilities was highly dependent on interagency cooperation.
- In 2000, the NIPC drafted the *National Infrastructure Protection Center Priorities and Goals 2000-2002* document, which was intended for approval and input from a proposed advisory board. The document contains an outline of goals and objectives for analysis and warning capabilities, but does not address the interim steps needed to achieve them.
- In 2000, the Analysis and Warning Section developed seven detailed goals and related objectives for fiscal year 2001. However, this document did not provide an explanation or strategy on how NIPC would achieve them.
- NIPC officials provided us documents they say were used to support their 1999, 2000, 2001 budget requests for analysis and warning efforts. These documents identify resources, strategies and current shortfalls.

While these documents provide information on the NIPC's general plans and needed resources, the information is fragmented and incomplete. As a result, it does not provide a comprehensive road map to guide, communicate, and measure progress. Such plans are also important because they serve to clarify and communicate objectives and goals. In addition, the plans can highlight potential problems, describe resource needs, and provide a means for measuring performance. The Government Performance and Results Act of 1993[6] required federal agencies to develop strategic plans that included six key elements. Although that act does not

[6]P. L. 103-62, August 3, 1993, sec. 3 (5 U.S.C. 306).

require such plans for individual agency programs, the following six key elements it identifies serve as a useful guide:

- a comprehensive agency mission statement;
- general goals and objectives for all major functions and operations;
- a description of how the goals and objectives are to be achieved, including operational processes, skills, and technology and the human capital and other resources needed;
- a description of the relationship between the general goals and objectives and annual performance goals;
- identification of key factors, external to the agency and beyond its control, that could significantly affect the achievement of the general objectives and goals; and
- a description of how program evaluations were used to establish or revise general objectives and goals, and a schedule for future program evaluations.

The documents described above contained some of these elements; however, they did not (1) establish milestones and performance measures; (2) describe the specific operational processes, skills, and technology necessary to achieve the stated goals and objectives; (3) describe the relationship between the general goals and objectives and annual NIPC performance goals; and (4) describe how program evaluations would be used to establish or revise general objectives and goals and a schedule for future program evaluations.

Changes to NIPC Responsibilities Being Considered

At the close of our review, in February 2001, the National Coordinator told us that the administration had begun to consider options for adjusting the federal strategy for critical infrastructure protection originally outlined in PDD 63. He said that adjustments being considered included provisions related to the development of analysis and warning capabilities currently assigned to the NIPC and that one intent of any such changes would be to clarify roles and responsibilities in this area.

Conclusions

While the NIPC has taken some steps to develop analysis and warning capabilities, the strategic capabilities described in PDD 63 have not been achieved. Many of the factors that have impeded the NIPC's progress in this area, such as the absence of a methodology for strategic threat analysis, the lack of needed staff and expertise, and inadequate data on infrastructures, will require coordinated information-sharing and analysis

efforts by the federal agencies that have pertinent expertise. Similarly, the NIPC efforts in warning have also been impeded by the lack of a comprehensive, governmentwide data-collection framework for identifying imminent computer-based attacks. Further, the NIPC faces other barriers in issuing timely warnings, including a shortage of skilled staff, avoiding undue alarm for insignificant incidents, and ensuring that sensitive information is protected.

Evaluating the NIPC's progress is difficult because its roles and responsibilities have not been fully defined and are not consistently interpreted by other entities responsible for critical infrastructure protection. Specifically, it remains unclear who has direct authority for the NIPC and if the NIPC is to be integrated into the national security warning process. Further, no criteria have been developed for determining when a computer-based incident threatens national security and what related protocols would be used to place the NIPC in support of DOD or the intelligence community. Clarifying such issues and engendering governmentwide support and assistance will be important elements of ensuring the successful development of the analysis and warning capabilities envisioned by PDD 63. In addition, developing a comprehensive, integrated plan to guide activities related to establishing analysis and warning capabilities, outline related resource needs, and identify impediments to progress would provide valuable input for consideration as the government moves forward with efforts to protect critical infrastructures.

Recommendations for Executive Action

On the basis of the criteria provided in PDD 63 and related plans, we recommend that the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategic analysis of computer-based threats, including developing a related methodology, acquiring staff expertise, and obtaining infrastructure data;
- develop a comprehensive governmentwide data-collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and
- clearly define the role of the NIPC in relation to other government and private-sector entities, including
  - lines of authority among the NIPC and the National Security Council, Justice, the FBI, and other entities;

- the NIPC's integration into the national warning system; and
- protocols that articulate how and under what circumstances the NIPC would be placed in a support function to either the DOD or the intelligence community.

We recommend that the Attorney General task the FBI Director to require the NIPC Director to develop a comprehensive written plan for establishing analysis and warning capabilities that integrates existing planning elements and includes

- milestones and performance measures;
- approaches (or strategies) and the various resources needed to achieve the goals and objectives;
- a description of the relationship between the long-term goals and objectives and the annual performance goals; and
- a description of how program evaluations could be used to establish or revise strategic goals, along with a schedule for future program evaluations.

Agency Comments and Our Evaluation

In commenting on a draft of this report, the Director of the NIPC generally agreed with the report's findings and stated that the NIPC considers it of the utmost urgency to address the shortcomings identified. The Director expressed the view that it is most important that the NIPC receive adequate staffing, particularly from the defense and intelligence communities, to address the lack of strategic analysis. In particular, the Director said that the report should reflect that many executive branch components had not heeded the call set out in PDD 63 to "provide such assistance, information and advice that the NIPC may request." In addition, the Director recommended that the report recognize the NIPC's performance in the context of its recent formation, noting that the NIPC has been in existence for only 3 years. Finally, the Director noted that our report did not recommend a change to the basic PDD 63 framework. In this regard, he expressed the view that the FBI is the only locus where law enforcement, counterintelligence, foreign intelligence, and private-sector information may be lawfully and collectively analyzed and disseminated, all under well-developed statutory protections and oversight of the Department of Justice. The Director's letter did not comment on our recommendations to the NIPC regarding the need for a comprehensive, integrated plan for developing analysis and warning capabilities.

The NIPC's comments regarding the need for additional staff largely reiterate our findings, which note that the NIPC has not received the anticipated number of detailees from other executive departments. In addition, our report repeatedly notes that the NIPC was established in early 1998. We have no additional information to add on these two topics. Further, as the NIPC Director states, we did not recommend a change to the basic PDD 63 framework, including changing the placement of the NIPC. We did not make such a recommendation because moving the NIPC from the FBI to another agency or establishing it as a stand-alone entity would not necessarily ensure that the deficiencies we identified would be addressed. These deficiencies, which included lack of a generally accepted methodology for strategic analysis, lack of data on infrastructure vulnerabilities and incidents, and insufficient staff resources, are problems that need to be addressed regardless of the NIPC's organizational placement.

The Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council also provided comments, saying that our report highlighted the need for a review of the roles and responsibilities of the federal agencies involved in U.S. critical infrastructure protection support. The comments stated that the administration will consider our recommendations as it reviews federal cyber activities to determine how the critical infrastructure protection function should be organized. The Special Assistant to the President noted that some functions might be better accomplished by distributing the tasks across several existing federal agencies, creating a "virtual analysis center" that would provide not only a governmentwide analysis and reporting capability, but that could also support rapid dissemination of cyber threat and warning information.

The comments from the NIPC and the National Security Council are printed in full in appendixes I and II, respectively.

The NIPC Has Provided Valuable Support and Coordination in Improving Investigation and Response Capabilities

PDD 63 directed the NIPC to provide the principal means of facilitating and coordinating the federal government's response to computer-based incidents, mitigating attacks, and monitoring reconstitution efforts. In response, the NIPC has undertaken efforts in two major areas.

First, the NIPC has provided coordination and technical support to FBI field offices, which have established special squads and teams and one regional task force to address the growing number of computer crime cases. The NIPC's support has provided benefits, but activities in several areas have not yet met expectations outlined in the FBI's April 1999 *National Infrastructure Protection and Computer Intrusion Program Plan*. For example, insufficient computer capacity and data transmission capabilities have limited the NIPC's ability to perform technical analyses quickly. In addition, FBI field offices are not yet providing the NIPC with the comprehensive information that NIPC officials say is needed to facilitate prompt identification and response to such cyber incidents.

Second, the NIPC has developed crisis management capabilities to support a multiagency response to the most serious incidents. Procedures for establishing crisis-management teams have been developed and, on the basis of experience with actual incidents, refined. In addition, the NIPC has developed a draft emergency law enforcement sector plan to guide the response of federal, state, and local entities. As of mid-February 2001, the draft plan was being reviewed by law enforcement sector members.

Regarding the requirement that the NIPC develop capabilities to "monitor reconstitution" of computer systems, NIPC officials told us that virtually nothing has been done because specific expectations for the NIPC in this area have not been defined. The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism agreed that the NIPC's specific role in this area was not clear and said that this issue would probably be addressed as the administration reviews the government's critical infrastructure protection strategy and the specific requirements of PDD 63.

The NIPC Has Provided Coordination and Technical Support to FBI Field Squads

Since 1998, FBI investigative units and the NIPC have worked together to address the growing number of computer crime cases, which federal law enforcement guidelines define as attacks on computer systems for the purpose of acquiring information or to damage or disrupt the target computer system. Such cases do not include computer-facilitated crimes, such as Internet fraud, e-mail extortion, or child pornography, which are

handled by other FBI investigative programs. The NIPC's support has provided benefits, but activities in several areas have not yet met expectations outlined in the *National Infrastructure Protection and Computer Intrusion Program Plan*.

Increase in Computer Crime Cases Has Prompted the Need for Increased Coordination and Technical Support

According to the FBI Director and NIPC officials, the number of computer crime cases more than doubled from fiscal years 1998 to 2000, as shown in table 2. NIPC officials estimate that the number of pending cases for such crimes will increase to 3,150 by fiscal year 2002.

Table 2: Computer Crime Cases From FY 1998 to FY 2000 (all numbers are as of October 1)

Case status	FY 1998	FY 1999	FY 2000
Opened	540	801	1,132
Closed	399	912	834
Pending	453	795	1,123

Source: NIPC officials.

In addition to increasing in numbers, computer crime cases tend to be technically complex and resource-intensive to investigate, frequently involving more than one state or nation and often requiring coordination of efforts by many FBI field offices and other law enforcement entities. In February 1998, one such multiagency investigation demonstrated the need for an interagency center like the NIPC to coordinate investigative activities that relate to potentially serious intrusions. The investigation, referred to as Solar Sunrise, involved a series of related intrusions into more than 500 military, civilian government, and private-sector computer systems. Because the intrusions took place during the build-up of U.S. military personnel in the Middle East in response to tensions with Iraq and because the source of the intrusions could not immediately be determined, the episode raised serious national security concerns. The FBI worked closely with Israeli law enforcement authorities to solve the case, and, within several days, the investigation determined that juveniles in California and individuals in Israel were the perpetrators.

Other cases illustrating the need for coordination include investigation of the ILOVEYOU virus in 2000, which involved 50 FBI agents from various locations and coordination with the government of the Philippines, and

investigation of a denial-of-service attack in late 1999, which involved 36 FBI field offices and 13 legal attachés, who are FBI agents stationed abroad. In addition, the cases identified in table 2 include 12 foreign counterintelligence cases, which, according to NIPC officials, usually require more time-consuming technical analysis—2 such cases took over 18,000 hours of analysis. At the end of fiscal year 2000, over 15 percent of the 1,123 pending computer crime investigations were being conducted jointly with other investigative agencies.

FBI Field Squads and Regional Task Force Established to Facilitate Investigations

In October 1998, the FBI created the National Infrastructure Protection and Computer Intrusion Program to strengthen its ability to investigate computer-based attacks on critical infrastructures and tasked the NIPC to provide administrative and operational support. The program called for the establishment of special squads, referred to as NIPC squads, in the FBI field offices to serve as centers of expertise for investigating computer crime. The *National Infrastructure Protection and Computer Intrusion Program Plan* set a goal of establishing an NIPC squad in each FBI field office by 2003.

As of December 31, 2000, the FBI had established such squads, each consisting of approximately 8 FBI agents, in 16 of the FBI's 56 field offices. In addition, 40 smaller teams of from 1 to 5 agents, dedicated to working computer crime cases, have been established in other FBI field offices. These squads and teams have served as focal points for computer crime investigations in their regions. The number of agents assigned to the NIPC squads has increased from 76 agents in fiscal year 1998 to approximately 200 agents in fiscal years 1999 and 2000, most of these agents were transferred from other FBI investigative programs.

While the NIPC provides support and coordination, the NIPC squads are under the FBI field offices' direct supervision. Accordingly, the field offices determine when a case is to be opened and whether an incident needs to be referred to other federal, state, or local law enforcement entities. In addition, FBI field offices are usually the first to be alerted to potential computer crime cases, most often by victims or informants. Generally, the NIPC becomes involved when notified by the field squads through case-initiation paperwork, requests for technical assistance or direct notification by telephone.

The *National Infrastructure Protection and Computer Intrusion Program Plan* also called for the NIPC field squads to establish interagency task

forces to coordinate investigative work and facilitate information sharing and coordinate investigations regarding computer crimes with other law enforcement entities. As of December 31, 2000, only one task force had been created. However, NIPC officials expected the task force to serve as a model for similar task forces in other locations.

Comprising representatives from Justice, the U.S. Postal Service, Secret Service, Defense Criminal Investigative Service, Internal Revenue Service, and state and local law enforcement entities, the task force was established in March 2000 in the FBI's Pittsburgh field office. Since then, the task force has undertaken several efforts that NIPC officials and task force members agree have improved computer crime investigative capabilities in that region. For example, the task force has

- investigated 28 cases jointly with other law enforcement entities—accounting for approximately 15 percent of the FBI's 177 joint computer crime cases;
- briefed other members of the law enforcement community and private industry on investigative techniques, including the handling of electronic evidence related to computer crime;
- sponsored development of a computer laboratory to facilitate collaboration on investigations and leverage resources donated by member agencies, including computers and analytical tools; and
- served as a forum for discussing common challenges and issues.

NIPC Support Has Provided Benefits

The NIPC has benefited computer crime investigations by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases; (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks; and (3) providing administrative support to NIPC field agents. For example, the NIPC reports that it has

- produced over 250 written technical reports[1] during 1999 and 2000, over 80 percent of which supported investigations led by other law enforcement agencies;

[1]These technical reports were developed as part of computer intrusion investigations and focus on the technical attributes of the intrusion, including the vulnerabilities exploited and steps taken during the intrusion. This focus on the specific details of individual investigations distinguishes these technical reports from the analytical reports produced by the AISU and discussed in chapter 2 of this report.

- responded to an average of six requests per day for technical analysis;
- developed analytical tools—some of which are classified—to assist in investigating and mitigating computer-based attacks, including both original software and modified commercial software;
- created and posted software tools, including tools issued in December 1999 and May 2000, for detecting the presence of denial-of-service software, one of which was downloaded 1,200 times in one 24-hour period, indicating that it was widely used;
- managed the procurement and installation of hardware and software tools for each of the NIPC field squads and teams;
- managed development of a data warehousing project, referred to as the Early Warning System, which is intended to link numerous sources of electronic information so that they can be searched as a single entity, thereby facilitating searches and accelerating investigations—a capability that, according to officials, will also benefit tactical and strategic analysis;
- provided legal guidance and coordination with Justice units and assisted in obtaining the necessary court orders to conduct data intercepts;
- analyzed case-initiation paperwork to identify cases with similarities so that they could be coordinated;
- identified and shared improved investigative techniques regarding computer crime; and
- streamlined administrative procedures for the increasing number of foreign counterintelligence cases, such as the recent investigations into the possible theft of nuclear secrets from the Los Alamos National Laboratory.

Examples of significant cases that the NIPC has coordinated or supported include the following:

- In March 1999, the NIPC coordinated the FBI field office investigation into the Melissa macro virus, which caused an estimated $80 million in losses. Although the Melissa virus did not actually destroy or alter data, it generated large volumes of e-mail that congested and shut down computers. Within less than a month, the virus' author was arrested.
- In June 1999, the NIPC coordinated an investigation of a Trojan horse virus, referred to as the Explore.Zip worm, with six FBI field offices. The virus had infected various private-sector computer systems and propagated through the Internet via an e-mail attachment, destroying certain files on computer hard drives. At the close of our review, the investigation had been ongoing for over a year.

- From January to March 2000, the NIPC supported an investigation of two teenagers who had used a computer in the United Kingdom to break into e-commerce sites in five countries and steal information resulting in estimated losses totaling over $3 million. The case, referred to as "Curador," was based on investigative work by the FBI and police in the United Kingdom and Canada. The perpetrators were arrested and charged in the United Kingdom in March 2000.

Problems Affecting the NIPC's Effectiveness in Supporting Investigative Efforts

The *National Infrastructure Protection and Computer Intrusion Program Plan* and the NIPC budget justifications identified several deficiencies that are impeding the NIPC's ability to coordinate and support investigations of computer crime cases. First, according to NIPC officials, delays had occurred because the NIPC's Special Technologies and Applications Unit did not have computers capable of rapidly analyzing the large amounts of data associated with some cases. Recent investigations have required the unit to collect and analyze multiterabytes of data (equivalent to one or more times the amount of information contained in the Library of Congress). However, to analyze these data on its existing equipment, they must be broken into segments and examined separately because the unit's computer capacity was insufficient to handle the large amount of data. According to NIPC officials, the inadequacy of its current computer system is contributing to a 30-day backlog in meeting requests for analysis from the field offices.

In addition, agents in some field offices told us that they lack the means to securely transmit large amounts of data between field offices and the NIPC for analysis. These factors prolong the time needed to transmit and analyze data and have contributed to the backlog of analyses that need to be performed. According to NIPC officials and internal budget documents, funding for additional computer equipment will be requested for fiscal year 2002.

Further, NIPC field squads are not reporting all of the information they have on unusual or suspicious computer-based activity to the NIPC. The *National Infrastructure Protection and Computer Intrusion Program Plan* states that it is imperative that all field offices document and report all complaints regarding computer intrusion activity and forward the information to the NIPC. NIPC officials told us that receiving such comprehensive information provides the NIPC with a broader and more complete view of suspicious and unusual activity and facilitates prompt identification of potentially widespread problems. Such information is of

value to the NIPC's analysis and warning functions as well as its support of NIPC investigations. However, NIPC field squad members told us that minor incidents that did not merit opening a case were not always reported to the NIPC because many incidents were deemed to be insignificant.

To provide an increased incentive for sharing information, the NIPC established new performance measures for fiscal year 2001 so that field squads receive credit for the amount of information shared about potential cyber incidents, regardless of whether or not a case is opened.

Crisis Management Plans Have Been Developed

According to the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan,* as the lead entity responsible for coordinating the federal government's crisis management and response to computer-based attacks, the NIPC must be able to respond quickly in the initial stages of a crisis situation and pursue the appropriate law enforcement or national security strategies. The NIPC's primary efforts to fulfill these responsibilities have been related to developing procedures for implementing crisis action teams in response to computer-based attacks and intrusions. Since 1998, the NIPC has formed seven such teams, comprising a combination of NIPC personnel—agents and detailees, which have responded to a range of classified and unclassified events lasting from a day to over a year. Generally, these teams have served as the focal point for coordinating the investigation and response to incidents with national impact, including the Melissa virus in April, May, and June 1999; the transition to the year 2000; and denial-of-service attacks in February and March 2000. In 1999, the FBI established an expanded Strategic Information Operations Center, a crisis management center at FBI headquarters, which has provided the teams with a collaborative working environment and access to information through computer and telecommunications support.

In August 2000, the NIPC standardized its procedures for initiating crisis action teams and developed a detailed concept of operations to guide future response. The detailed document identifies thresholds for activating crisis teams, delineates the missions of the team members, and provides a framework for involving individuals from the NIPC and other agencies.

In addition, the NIPC has drafted an emergency law enforcement sector plan. PDD 63 designated Justice and the FBI as the lead agencies for the emergency law enforcement services sector, and the FBI delegated this responsibility, including development of the sector plan, to the NIPC. The

plan covers the roles and responsibilities for the more than 18,000 law enforcement agencies throughout the United States that the NIPC says have volunteered to participate. In addition, the plan describes approaches for assessing the vulnerability of critical law enforcement systems, developing remediation and mitigation plans, and improving awareness of law enforcement personnel. As of mid-February 2001, the NIPC had provided the draft plan to sector members and was awaiting their comments.

In addition to the NIPC's crisis management efforts, in July 2000, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism created two new entities involving the NIPC that are designed to improve federal policymaking and response to computer-based attacks. The Cyber Incident Steering Group is responsible for determining the appropriate policy for response, and the Cyber Incident Working Group is responsible for executing and coordinating a response. The National Coordinator chairs the steering group, of which the NIPC Director is a member, while the NIPC Director chairs the working group.

According to a process defined by the National Coordinator, the NIPC Director is to convene the working group when an unauthorized cyber event occurs that has a significant national security, economic, or public safety impact. The working group is primarily to share information on specific incidents and discuss related mitigating actions. In addition to the NIPC Director, the group's membership includes the Commander of the Joint Task Force for Computer Network Defense, U.S. Space Command; the Program Director of the Federal Computer Incident Response Capability, the General Services Administration (GSA); and the Chief, Defensive Information Operations Group at the National Security Agency. Other agency representatives may be added, as appropriate. At the close of our review, the Cyber Incident Working Group had convened once, in November 2000, to discuss issues related to hostile computer-based activity in the Middle East.

Requirements for Monitoring Reconstitution Have Not Been Defined

PDD 63 states that there will be a system to rapidly reconstitute the minimum required capabilities after an infrastructure attack, and it specifically assigns the NIPC responsibility for monitoring reconstitution. The National Plan states that the NIPC's responsibility in this area includes monitoring reconstitution of telecommunications and computer networks on which the government relies.

NIPC officials told us that they have not planned or taken any action in this regard because specific expectations for meeting the requirements briefly mentioned in PDD 63 and the *National Plan* have not been further defined. As a result, while the NIPC has established procedures for crisis management teams, previously discussed, it is not clear what responsibilities these teams would have regarding any reconstitution efforts that may be needed as the result of a seriously damaging attack.

The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism agreed that the NIPC's specific role in this area was not clear and said that this issue would probably be addressed as the administration reviews the government's critical infrastructure protection strategy and the specific requirements of PDD 63.

Conclusions

The NIPC has provided important support in increasing the FBI's ability to investigate computer crimes by coordinating investigations and providing technical assistance. However, at some locations, insufficient computer and communications capabilities have hindered the NIPC's ability to promptly and efficiently analyze large amounts of data in support of investigations, and FBI field office personnel are not providing the NIPC with all of the information they have on potentially damaging or hostile computer-based activity. The NIPC has also developed crisis management procedures and drafted an emergency law enforcement sector plan, which is currently being reviewed by sector members. In 2000, the National Coordinator supplemented these efforts by establishing the Cyber Incident Steering Group, to develop response policies, and the Cyber Incident Working Group, which is responsible for executing and coordinating a response. No actions had been taken to develop capabilities to monitor reconstitution of computer systems because specific expectations for the NIPC in this area have not been defined.

Recommendations for Executive Action

To ensure that the NIPC develops the response, investigative, and crisis management capabilities required by PDD 63, we recommend that the Attorney General direct the FBI Director to task the NIPC Director to

- ensure that the Special Technologies and Applications Unit has access to the computer and communications resources necessary to analyze data associated with the increasing number of complex investigations;

- monitor implementation of new performance measures to ensure that they result in field offices' fully reporting information on potential computer crimes to the NIPC; and
- complete development of the emergency law enforcement plan, after comments are received from law enforcement sector members.

As the national strategy for critical infrastructure protection is reviewed and possible changes considered, we recommend that the Assistant to the President for National Security Affairs define the NIPC's responsibilities for monitoring reconstitution.

Agency Comments and Our Evaluation

In commenting on a draft of this report, the Director of the NIPC expressed the view that, despite formidable hurdles, the NIPC has achieved remarkable success, noting the establishment of a nationwide program for investigating computer crime in 56 FBI field offices. He also said that the NIPC, in conjunction with the Emergency Law Enforcement Sector Forum, had developed the only sector infrastructure protection plan, which was delivered to the National Coordinator in March 2001. The Director's comments did not address our recommendations to the NIPC regarding the need to (1) ensure that the Special Technologies and Applications Unit had access to adequate computer and communications resources and (2) monitor implementation of new performance measures regarding field office reporting of information on potential computer crimes.

Our report describes the National Infrastructure Protection and Computer Intrusion Program, under which NIPC units in 56 FBI field offices have been established, and the report commends the NIPC for providing valuable coordination and technical support to this program. Our report also credits the NIPC with leading development of the Emergency Law Enforcement sector plan. We did not review the progress of other infrastructure sectors in developing similar plans because such efforts were not within the scope of our review. As a result, we cannot compare progress on the Emergency Law Enforcement sector plan with progress on similar plans for other infrastructure sectors.

In commenting on a draft of this report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council said that our comments would be considered as the administration reviews federal cyber activities to determine how the critical infrastructure protection function should be organized. The

comments did not specifically address our recommendation that the NIPC's responsibilities for monitoring reconstitution be defined.

The comments from the NIPC and the National Security Council are printed in full in appendixes I and II, respectively.

Progress In Information Sharing And Outreach Has Been Mixed

To help ensure that computer-based attacks are promptly detected and that mitigation and recovery efforts are effective, PDD 63 calls for extensive cooperation and information sharing among government and private-sector entities. According to the January 2000 *National Plan for Information Systems Protection,* the role of the federal government is to (1) create federal capabilities for enhanced information sharing and (2) encourage nonfederal entities (the private sector and state and local governments) to organize themselves for efficient information exchange about cyber threats and incidents. The *National Plan* further states that "the NIPC has a vital role in collecting and disseminating information from all relevant sources" and that it is to accomplish this by "establishing a network of relationships with entities in both the government and the private sector."

Since 1998, the NIPC has undertaken a range of initiatives designed to foster information sharing among private-sector, government, and international entities with mixed results. Regarding the private sector, the NIPC has developed a collaborative relationship with the electric power industry, but two-way information-sharing relationships between the NIPC and other information-sharing and analysis centers has not developed. In addition, the NIPC has increased the membership of its InfraGard Program, which is designed to build direct relationships with individual companies, but has made limited progress in developing its Key Asset Initiative, which is designed to create a database of critical infrastructure components, including those that are privately controlled.

NIPC efforts to establish information-sharing and coordination relationships with other government entities have met with less success. Federal agencies have not routinely reported incident information to the NIPC, DOD and the NIPC agree that their information sharing needs improvement, and Secret Service expertise has not been integrated into the NIPC efforts. However, NIPC efforts to provide training on investigating computer crime, which it views as an element of its outreach efforts, have involved an increasing number of personnel from federal, state and local, and international entities, and the NIPC has participated with several other countries in infrastructure protection efforts.

Information Sharing And Coordination Are Essential To Combat Cyber Attacks, But Present Challenges

Information sharing and coordination among organizations are key elements in developing comprehensive and practical approaches to defending against cyber threats. Having information on threats and actual incidents experienced by others can help an organization better understand the risks it faces and determine what preventive measures should be implemented. In addition, prompt warnings can help an organization take immediate steps to mitigate an imminent attack. Information sharing and coordination are also important after an attack, to facilitate recovery and criminal investigations.

In July 2000,[1] we testified on the importance of information sharing on cyber threats and related challenges, noting that creating partnerships for information sharing and coordination is a formidable task. Most important, trust must be established among parties who may have varying interests and expectations. For example, private-sector entities are usually motivated by business concerns and profits, whereas governments are driven by national and economic security concerns. These disparate interests can lead to profoundly different views and perceptions about threats, vulnerabilities, and risks, and they can affect the level of risk each party is willing to accept and the costs each is willing to bear. Further, the private sector may have reservations about sharing information with law enforcement agencies because compliance with law enforcement procedures can be costly, or a business may not wish to report an incident that might tarnish its image. Government entities, on the other hand, may be reluctant to share information for national security reasons, and declassifying and sanitizing such data takes time and could delay response. In addition to developing trust relationships, reporting needs and mechanisms for sharing are necessary to ensure that the right type of information is provided and that effective and secure procedures are in place for handling the information. This effort requires agreeing, in advance, on the types of data to be collected and reported and the processes to be used.

[1] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation* (GAO/T-AIMD-00-268, July 26, 2000).

Information-sharing Success With Private Sector Has Varied

To improve communication and information sharing with private-sector entities, the NIPC has

- attempted to establish relationships with ISACs for individual infrastructure sectors;
- established a mutually beneficial relationship with CERT/CC;
- expanded the FBI's InfraGard Program to facilitate secure information sharing with individual entities; and
- begun developing a database of key infrastructure components, referred to as the Key Asset Initiative.

All of these efforts are in relatively early stages of development, and their success to date has varied.

The NIPC Has Developed Two-Way Information Sharing With One Industry Sector

PDD 63 introduced the concept of establishing a private-sector ISAC to gather and analyze industry-provided information on threats and incidents and share this information with government entities. The *National Plan* detailed the government's plans in this area, on the basis of discussions held with government and industry officials, encouraging establishment of ISACs for major industry sectors. The *National Plan* noted that ISACs could serve as a means of (1) sharing information on attempted intrusions and attacks with industry partners and government entities and (2) obtaining warning information from the government. Specifically, the *National Plan* stated that the NIPC would use the ISACs as a means of disseminating information to industry sectors. It also encouraged private companies to inform federal agencies about attempted intrusions and attacks, possibly by reporting through the ISACs. However, it stated that such reporting was voluntary. Details of the ISACs' design and operations were to be determined by the private sector, in consultation with and with assistance from the federal government.

During 1999 and 2000, ISACs were established for the financial services and telecommunications sectors. In addition, the North American Electric Reliability Council recently formally declared itself the electric power industry ISAC, although it had functioned in this fashion for some time. Another ISAC, for the information technology industry, was announced by the Secretary of Commerce on January 16, 2001, just prior to the close of our review.

Collaboration With Electric Power Industry Illustrates Value of Public-Private Coordination

According to NIPC and industry officials, the "Indications, Analysis and Warning Program" established with the North American Electric Reliability Council on behalf of the electric power industry has provided useful information to both the NIPC and the industry sector and may prove to be a model for future efforts in other industry sectors. The relationship between the NIPC and the council has been successful, in part, because the electric power industry has had a history of working directly with the FBI, so there was an existing relationship on which to build. The council is made up of 10 regional councils from all segments of the electric industry—investor-owned, federal, rural electric cooperatives, state/municipal and provincial utilities, independent power producers, and power marketers. Its members control virtually all of the electricity supplied in the United States, Canada, and Mexico.

In March 1999, the NIPC and the council began the Indications, Analysis, and Warning Program with the intention of developing standard methods for sharing and reporting information. By October 1999, they had initiated a pilot program to test these methods and develop thresholds for incident reporting. The council encourages the electric utility companies to voluntarily provide the NIPC with information on unscheduled service outages, degraded operations, and serious threats to facilities, activities, and information systems, according to agreed-upon methods and criteria. The agreement also stipulated requirements for the NIPC's handling of incident reports. For example, the NIPC is to log all reports immediately and acknowledge receipt to the report's originator. The NIPC then is to record the report in an incident database and make it available to others only in accordance with established protocols. In October and November 2000, the NIPC held training conferences with the electric power industry on general guidelines for electric utility companies to follow in voluntarily reporting information to the NIPC.

According to NIPC and council officials, in addition to establishing an information-sharing mechanism, the program has better defined the NIPC's information needs and provided industry members with information on vulnerabilities and threats that they may not have otherwise obtained. For example, in December 2000, information gathered through the electric power industry led to detection of a potentially damaging computer exploit and issuance of a warning to industry members and the public.

Two-Way Communication Between the NIPC and Other ISACs Has Not Developed

Establishing a two-way means of communication with the telecommunications and financial services ISACs has been less successful. Although both ISACs receive information from the NIPC, neither has

provided information in return because of reporting incompatibilities and concerns about confidentiality.

The telecommunications ISAC was officially recognized in a January 2000 memorandum from the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. This ISAC is a consortium of private carriers and federal agencies, but it is managed by the National Communications System, an interagency entity established in the early 1960s to ensure reliable communication for the government in all situations.

According to National Communications System officials, the telecommunications ISAC has received information from the NIPC, including telephone calls and electronic alerts, which the ISAC, in turn, has distributed to its membership. However, as of December 2000, these officials said that the ISAC had not shared any incident reports with the NIPC because ISAC members had not identified anything that was deemed important enough to share, noting that the NIPC and the telecommunications ISAC have not agreed to any thresholds for reporting incidents such as those established with the electric power industry. Furthermore, no standard thresholds have been developed between the telecommunications ISAC and its member companies. During attempts to develop criteria for reporting thresholds, the companies determined that it was not currently possible due to differences in internal operational thresholds and network monitoring software.

The Financial Services ISAC's objective is to help ensure the viability and continuity of the banking and finance sector from any intentional acts that could impact critical services or the orderly functions of the economy. Formed in October 1999, the financial services ISAC provides a data collection and analysis center, which is managed by a private contractor and funded by participating corporations and is structured to provide a globally distributed analytical capability that enables broad access to current information.

According to its operating rules established in April 2000, information on threats and vulnerabilities from government or law enforcement sources may be accepted by the ISAC. However, this is a one-way transfer of information. According to ISAC documents, the ISAC is for the exclusive use of the banking, securities, and insurance industries, and no U.S. government entity can access its resources. As a result, the NIPC has not benefited from information that it could have used to alert others. For

example, officials at both organizations told us that the financial services ISAC knew about the May 2000 ILOVEYOU virus hours before the NIPC, but the ISAC did not warn the NIPC.

The NIPC Has Begun a Mutually Beneficial Relationship With CERT/CC

An additional information-sharing relationship has been established between the NIPC team at the FBI's Pittsburgh Field Office and CERT/CC. Although not an industry-related ISAC, CERT/CC, funded primarily by DOD, is involved in gathering, analyzing, and sharing information on computer-based vulnerabilities with private- and public-sector entities. In April 1999, the NIPC team in Pittsburgh assigned an agent to work with CERT/CC for 18 months. According to CERT/CC personnel, having a law enforcement officer work with them helped them better understand the legal issues, including standards of evidence, involved in dealing with a computer attack or compromise and allowed them to better advise their clients in this regard, including collaborating on an evidence handling paper with the CERT/CC in July 2000. In addition, they said, the NIPC team provided technical information about a recent denial-of-service attack that helped CERT/CC develop a better solution.

InfraGard Program Has Expanded Nationwide

To facilitate information sharing directly with individual private-sector entities, the NIPC adopted and expanded the InfraGard Program, which had begun in 1996 in the FBI's Cleveland Field Office as a pilot project. According to InfraGard documents, the program is intended to establish a secure mechanism for electronic two-way information sharing about intrusion incidents and system vulnerabilities and a secure channel over which the NIPC can disseminate analytical reports on threats to private-sector entities. The *National Plan* provided more detailed objectives, stating that the InfraGard Program would

- provide members with prompt, value-added threat advisories, alerts, and assessments;
- increase the quantity and quality of infrastructure threat information and incident reports provided to local FBI field offices (for coordination, investigation, and follow up) and the NIPC (for national-level analysis and warning);
- increase interaction and information sharing among InfraGard members, their local FBI field offices, and the NIPC, on infrastructure threats, vulnerabilities, and interdependencies;

- ensure the protection of cyber and physical threat data shared among InfraGard members, FBI field offices, and the NIPC through compliance with proprietary, legal, and security requirements; and
- provide members with a forum for education and training on infrastructure vulnerabilities and protection measures.

By October 2000, 56 InfraGard chapters and subchapters had been established across the country with a membership of over 277 entities. In early January 2001, NIPC officials announced that membership had grown to 518 entities, including representatives from the FBI, private industry, other government agencies, state and local law enforcement, and the academic community.

InfraGard has two categories of membership—secure and nonsecure. According to NIPC records, as of September 2000, about 78 percent of InfraGard members had established secure memberships and could access the InfraGard Alert Network and secure Web page. Secure memberships require a background check verifying that applicants are not known computer hackers or criminals. Nonsecure members do not have access to these features, but they can attend meetings and fully participate in chapter activities. The large percentage of secure memberships may indicate that members value InfraGard participation. However, we did not interview InfraGard members, so we cannot comment on their satisfaction with the program.

NIPC officials have stated publicly that the InfraGard Program illustrates the success of their efforts in establishing trusted relationships with private-sector entities. In addition, the officials say the program has benefited efforts to combat computer-based attacks. For example, on the basis of information received from an InfraGard member, NIPC officials said they were able to warn approximately 100 companies about a possible computer attack that had been placed in their systems. However, agents in one field office expressed concern that the NIPC may not be able to support the InfraGard secure Web site with in-depth analysis, due to the deficiencies in the NIPC's analytical capabilities previously discussed in chapter 2. As a result, these agents said that they were concerned that InfraGard members' expectations may not be met.

Limited Progress in Identifying Key Assets

According to the *National Plan*, the Attorney General's plan, and the *National Infrastructure Protection and Computer Intrusion Program Plan*, the Key Asset Initiative was established to identify national, regional, and

local infrastructure components, such as certain telecommunications switching nodes, whose loss would potentially have widespread and dire social and economic consequences. Identifying such infrastructure components, or "key assets," would allow the NIPC and others involved in critical infrastructure protection to focus their analysis, protection, warning, and reconstitution efforts on the most important elements of the nation's infrastructure and facilitate recovery efforts should severe damage occur. In addition, such information is essential to understanding the significance of individual points of failure and assessing the potential criticality of an attack. Without this information, organizations may underprotect certain vital assets while overprotecting assets of lesser importance.

The NIPC and the NIPC squads at FBI field offices began identifying key assets and developing a related database in 1998 by building on previous FBI work, which had identified about 400 such assets. During 1999 and 2000, the NIPC hosted six training sessions, covering five industry sectors, for Key Asset Initiative coordinators, who are typically members of NIPC field squads and teams. According to training documents, agents in NIPC field squads are to conduct a thorough search for key assets in their regions for each of the eight major industry sectors. Then, the agents are to categorize the assets according to criteria provided. Once the list is developed, the agents are to contact the infrastructure owners or operators to ensure that all key assets have been identified. Lastly, they are to assist key asset owners in the development of contingency plans, if such plans do not exist.

At the close of our review, field squads had identified over 5,000 assets and categorized them as being of either national, regional, or local importance, as prescribed in NIPC training documents. However, our review of several segments of the database and related discussions with field squad personnel identified several indications that the field offices had not applied a consistent methodology in identifying assets. One agent told us that he had purposely omitted certain assets because, in his judgment, they were too sensitive to be included. Another agent told us he had used a telephone book as a primary source of identifying key facilities. In addition, there was great disparity between the number of assets identified for two large cities—over 800 assets had been identified for one city and only 34 for the other city. NIPC officials acknowledged that a process for reviewing database entries to ensure that FBI field offices are consistently applying the criteria outlined in training documents was needed but had not yet been implemented.

In addition, field squads had not yet been successful in obtaining the agreement of industry sectors regarding the importance of the assets they had identified because private companies have been hesitant to share information on their most critical assets. Such validation is important because many of the FBI agents who attempted to identify and rank infrastructure components did not have extensive industry knowledge.

Further, according to the Attorney General's plan, the Key Asset Initiative was to be developed in coordination with DOD and other agencies. Coordination among such efforts would help ensure that similar efforts underway at the NIPC and other agencies avoid inappropriate duplication of efforts and take advantage of the methods and findings that others have developed.

However, such coordination had not taken place. In particular, the Key Asset Initiative was not being coordinated with similar efforts in other agencies, primarily because agreements on sharing sensitive information had not been reached, as described below:

- NIPC officials held discussions with officials from Commerce's Critical Infrastructure Assurance Office regarding "Project Matrix," which is an effort led by that office to identify critical infrastructure components and related interdependencies affecting government operations. However, the officials did not reach any formal agreements to share information. An official involved with Project Matrix noted that the information gathered through Project Matrix efforts belonged to individual federal agencies and could not be shared without their express permission.
- NIPC and DOD officials exchanged multiple drafts of a memorandum of understanding regarding coordination between the NIPC and DOD's Joint Program Office for Special Technology Countermeasures and Infrastructure Assurance to identify infrastructure vulnerabilities that may affect DOD bases. However, the officials had not reached any agreements to share information as of December 2000.
- Officials with the National Communications System told us that they were approached by the NIPC about sharing information on important telecommunications components and facilities but declined because the industry provided such information for internal use only and to facilitate priority restoration during emergencies.

Senior NIPC officials agreed that much more needs to be done to validate the key asset database. They said that significant efforts to obtain industry

support and coordinate with other federal entities were not undertaken due to other priorities.

Information Sharing and Coordination With Other Government Entities Have Been Limited

PDD 63 directs other federal agencies to share information about threats and attacks with the NIPC, where permitted by law. However, as with the previously discussed efforts to identify key assets, the NIPC's broader efforts to share information and coordinate with government entities have not yielded significant results. Specifically, federal agencies have not routinely reported incident information to the NIPC, at least in part because OMB has directed civilian agencies to report incident information to GSA's Federal Computer Incident Response Capability, rather than to the NIPC. Also, DOD and the NIPC officials say that improved information-sharing agreements would be beneficial to their operations. Finally, the Secret Service withdrew the detailees it had originally provided to the NIPC because Secret Service officials felt that the Service's personnel were not provided appropriate responsibilities. The NIPC has been more successful in providing training to government entities, an effort that it considers to be an important component of its outreach efforts, and in coordinating with foreign governments that are establishing entities similar to the NIPC.

Recent Guidance Does Not Require Agencies to Report to the NIPC

The federal Chief Information Officers Council, which is chaired by OMB's Deputy Director for Management, has issued guidance to agencies on reporting incident and vulnerability information that is somewhat inconsistent with requirements outlined in PDD 63. Specifically, PDD 63 states the following:

"All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law."

In October 2000, the Chief Information Officers Council issued a memorandum, developed in cooperation with OMB and GSA, stating that agencies should share information on incidents and vulnerabilities with GSA's Federal Computer Incident Response Capability (FedCIRC), which, according to the *National Plan*, is to provide a means for federal agencies to work together to handle security incidents, share related information, solve common security problems, and collaborate with the NIPC and pertinent DOD entities. While the council's guidance did not preclude agencies from

reporting to the other organizations, it did not specifically require agencies to report to the NIPC. Specifically it stated that agencies "should contact FedCIRC as soon as they identify security incidents with origins external to the agency." Then, depending on the nature and severity of the incident reported, FedCIRC would provide further guidance, including determining if additional reporting to law enforcement or national security officials was appropriate.

This divergence in guidance reflects unresolved differences in the interpretation of NIPC's role in this area. Senior NIPC officials told us that they believe the guidance from the Chief Information Officers Council contradicts PDD 63's reporting requirements and that, in their view, FedCIRC's role as a focal point for federal reporting of computer-based incidents and vulnerabilities is a potentially detrimental and inefficient duplication of a portion of the NIPC's responsibilities. These officials would prefer that agencies report directly to the NIPC so that they can promptly integrate such information with intelligence and law enforcement information. NIPC officials believe that when agencies report first to another entity, such as FedCIRC, it compromises the NIPC's ability to promptly issue warnings and could result in unnecessary delay and damage should a serious incident occur. Conversely, OMB and FedCIRC officials have contended that FedCIRC is more focused on providing assistance and guidance to federal agencies and, therefore, is in a better position to respond to agencies' requests for assistance; analyze the initial information; and, if appropriate, forward it to the NIPC or others.

DOD and NIPC Information Sharing and Coordination Have Been Impeded by Lack of Formal Agreements

Both NIPC and DOD officials have identified the need to improve information sharing on their respective cyber-threat analysis efforts. The NIPC was designed to include a senior DOD manager to facilitate this process, and DOD's Deputy Assistant Secretary for Information Security and Operations said that, overall, the department has a good working relationship with the NIPC and the NIPC was very important to its efforts in this area. However, officials from both organizations said that a more structured process is needed.

DOD has significant efforts underway to gather and analyze threat and vulnerability data and to detect attacks against DOD computer systems that are either imminent or underway. For example, the Joint Task Force for Computer Network Defense, which is under the U.S. Space Command, monitors incidents and potential threats and coordinates across DOD to plan and direct actions to stop or contain damage and restore network

functionality. The task force's specific functions include (1) synchronizing technical, operational, and intelligence assessments of computer network attacks; (2) assessing and reporting impacts on military operations and capabilities; (3) coordinating the appropriate DOD actions to stop the attack and contain damage; and (4) coordinating, as required, with other government entities, including the NIPC, the private sector, and U.S. allies. Similarly, the National Security Incident Response Center, at the National Security Agency, provides warnings of threats and expert assistance to defense and civil agencies in isolating, containing, and resolving incidents that threaten national security systems. The center currently manages a database of computer incidents reported by DOD, other federal agencies, and many foreign sources.

NIPC officials maintain that they have had numerous discussions with DOD to develop formal requirements from defense specifying the type of information it wanted from the NIPC. However, no procedures or mechanisms have been developed to bring this about. An April 2000 memorandum from DOD's Director of Infrastructure and Information Assurance to the Assistant Secretary of Defense for Command, Control and Communications and Intelligence recommended several actions to facilitate information sharing and cooperation. These actions included

- establishing a more actively managed information clearinghouse and protocol to foster reciprocal exchanges of information and fulfill the NIPC's information-sharing mandate;
- ensuring that sensitive information is appropriately sanitized and handled;
- ensuring that the NIPC verifies incident reports pertaining to DOD with DOD prior to issuing the reports; and
- ensuring that the NIPC provides DOD with more information about all incidents, not just those directly affecting DOD, so that preventive measures can be implemented before DOD becomes a "victim."

To begin to address these concerns, DOD officials told us that they planned to develop a system for monitoring requests for information from the NIPC so that they could better assess the success of their responses, and NIPC officials said that they had asked DOD to develop specific information requirements.

Secret Service Not Adequately Integrated Into NIPC

According to PDD 63, the NIPC was to include FBI and Secret Service agents as well as other investigators with experience in computer crime and infrastructure protection. The Secret Service is authorized by statute to investigate fraud related to electronic fund transfers, credit cards, and identification documents. Accordingly, it has developed relationships with the financial services community and technical expertise, since 1987, through its Electronic Crimes Special Agent Program.

When the NIPC was formed in 1998, the Secretary of the Treasury requested seven positions in a letter to the Attorney General—a request with which the former NIPC director told us he agreed. Subsequently, two supervisory special agents from the Secret Service were assigned to the NIPC.

However, according to a June 2000 Secret Service letter to Senator Grassley and our interviews with Secret Service officials, contrary to Secret Service expectations, neither of the agents was allowed to participate in investigative activities or assigned responsibilities commensurate with their experience or grade. NIPC and Secret Service officials say that there were several attempts by both entities to discuss the issues, but satisfactory agreements were not reached. As a result, the Secret Service withdrew its detailees in October 1999, a factor that has contributed to the NIPC's shortage of skilled personnel. In November 2000, the Deputy Assistant Director for Investigations at Secret Service told us he maintains a liaison with the NIPC and that information sharing between the two entities was improving. However, as of December 31, 2000, no Secret Service detailees were assigned to the NIPC.

NIPC-sponsored Training Has Served as an Additional Element of Its Outreach Efforts

PDD 63 also required the NIPC to include training as part of its mission, and the *National Plan* noted that the NIPC was to provide training to federal, state, and local officials on infrastructure protection. In response, the NIPC has made training a key element of its outreach and information sharing to state and local entities. Since 1998, the NIPC has trained about 100 individuals from other federal agencies, as well as over 180 state and local government personnel, on investigating computer crime. Table 3 provides a summary of the number of personnel trained from May 1998 through August 2000.

Table 3: Personnel Trained by the NIPC From May 1998 Through August 2000

	Number of personnel who attended training		
Entities	FY 1998 (May 1998 – Oct . 1998)	FY 1999	FY 2000 (Oct. 1999 - Aug. 2000)
FBI	250	339	373
Other federal agencies	10	31	60
State and local	10	27	150
International	2	0	12
Total	**272**	**397**	**595**

Source: NIPC.

The NIPC Has Undertaken International Initiatives

The NIPC has worked on a range of international initiatives designed to foster better information sharing and communication across national borders. Since its founding in 1998, the NIPC has advised representatives from Canada, Germany, Japan, Sweden, and the United Kingdom, all of which are in the process of forming interagency entities like the NIPC. Also, in October 2000, the NIPC and the United Kingdom's National Infrastructure Security Coordination Center formed an operational subgroup to address (1) connectivity between the NIPC and the center, (2) coordination of outreach and information-sharing activities, and (3) ways to improve and accelerate the flow of information between the two entities and their respective partners.

Another international initiative that the NIPC has been involved in is a high-tech crime subgroup sponsored by eight major industrialized countries, including Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and Russia, collectively referred to as the G-8. An NIPC representative serves as a member of the U.S. delegation to the subgroup, which has been considering several issues concerning international cyber crime investigations, including the establishment of a 24-hour-a-day, high-tech crime network; international training conferences; reviews of legal systems in G-8 countries; and the development of principles on transborder access to stored computer data.

Finally, the NIPC has provided training to investigators from several nations through international law enforcement academies in Hungary and Thailand. In addition, a small number of select international investigators have received training in NIPC-sponsored classes in the United States.

During 2000, the NIPC records show that it participated in about 56 international events and provided briefings to visitors from 23 countries.

Conclusions

The NIPC's information-sharing relationships are still evolving and will probably have limited effectiveness until reporting procedures and thresholds are defined and trust relationships are established. While a growing number of entities have entered into information-sharing agreements with the NIPC and the FBI, two-way information-sharing partnerships have not developed between the NIPC and certain industry ISACs. This lack of cooperation impedes efforts to identify key assets that merit special protective efforts and identify and address vulnerabilities, and it increases the risk that a broad computer-based attack would not be detected or mitigated until significant damage had occurred. In addition, much work remains to develop cooperative relationships among government entities, including civilian agencies, DOD, and law enforcement entities, to ensure that similar or related critical infrastructure protection efforts are coordinated and that the expertise of agency personnel is used effectively.

Recommendations for Executive Action

To develop the information-sharing goals identified in PDD 63 and related plans, we recommend that the Assistant to the President for National Security Affairs (1) direct federal agencies and encourage the private sector to better define the types of information that are necessary and appropriate to exchange in order to combat computer-based attacks and procedures for performing such exchanges; (2) initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, such as those at DOD and Commerce; and (3) resolve discrepancies between PDD 63 requirements and guidance provided by the federal Chief Information Officers Council regarding computer incident reporting by federal agencies.

We further recommend that the Attorney General direct the FBI Director to direct the NIPC Director to (1) formalize relationships between the NIPC and other federal entities, including DOD and the Secret Service, and private-sector ISACs so that a clear understanding of what is expected from the respective organizations exists; (2) develop a plan to foster the two-way exchange of information between the NIPC and the ISACs; and (3) ensure that the Key Asset Initiative is integrated with other similar federal activities.

Agency Comments and Our Evaluation

In comments pertaining to this chapter, the Director of the NIPC recommended that our report more fully discuss the underlying causes that have led some in the private sector to offer limited or uneven cooperation with the government regarding the sharing of information related to infrastructure protection. The Director noted that each component in infrastructure protection operates under internal and external constraints on information sharing, which are based on important considerations in each component's mission. In this regard, he stated that Justice and the NIPC have worked, and will continue to work, to develop effective protocols for information sharing within the bounds of each component's legal and policy structures and provide a level of certainty that shared information will be appropriately protected. He asserted that, through such protocols, information necessary for protecting infrastructures can be effectively shared on a timely basis. He further cited several reasons why some private-sector organizations have been reluctant to share information with the government, including the NIPC. The reasons cited include (1) a lack of understanding or confidence in the exceptions found in the Freedom of Information Act, (2) concerns about whether Justice would pursue prosecutions at the expense of private-sector business interests, and (3) concerns about disclosing proprietary information to an entity beyond their control. The Director said that, to address these concerns, the NIPC has reached out to communities across the nation to build trust and educate the public on the legal and security aspects of information sharing and protection, citing the InfraGard Program and the NIPC's successful information-sharing relationship with the electric power ISAC. In addition, he cited two specific instances in which NIPC advisories were coordinated in advance with private-sector entities, including three ISACs, as evidence of the growing cooperative arrangement between the NIPC and the private sector. The Director did not specifically address our recommendations to the NIPC regarding the need to formalize relationships with other federal entities or ensure that the Key Asset Initiative is integrated with other similar federal activities.

The NIPC's comments reiterate many of the points made in our report regarding the challenges associated with building productive information-sharing relationships between private and public-sector entities, and they provide some additional specific detail. We agree that the underlying factors that inhibit information sharing are important, and our report cites our July 2000 testimony, which provides a much more detailed discussion of the related challenges. We also agree that the NIPC has taken a number of steps to address these concerns through the InfraGard Program and by

establishing cooperative relationships with the electric power ISAC and others. It is important that these efforts continue. In addition, as our report states, it is important that the NIPC strive for improved cooperative relationships with other federal entities involved in critical infrastructure protection.

In commenting on a draft of this report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council said that the administration will consider our recommendations as it reviews federal cyber activities to determine how the critical infrastructure protection function should be organized. The comments did not specifically address our recommendations regarding (1) better defining needed information for combating cyber attacks, (2) developing a strategy for identifying assets of national significance, and (3) resolving discrepancies in guidance on computer incident reporting by federal agencies.

The comments from the NIPC and the National Security Council are printed in full in appendixes I and II, respectively.

Funding Used For a Variety of NIPC-related Activities

Following congressional direction and on the basis of requirements estimated by NIPC officials, the FBI reportedly provided the NIPC with about $32 million and about $28 million for fiscal years 1999 and 2000, respectively. In addition, the FBI provided the NIPC with administrative services, including budgeting, accounting, training, telecommunications, and facilities, at no cost to the NIPC. Other government agencies provided the NIPC with additional resources in the form of at least 39 detailees over fiscal years 1999 and 2000. The detailees filled a variety of NIPC positions on a nonreimbursable basis.

On the basis of our analysis of information provided to us by the FBI Finance Division and the NIPC, the NIPC obligated about 84 percent of its available fiscal years 1999 and 2000 funds. The rest of the available funds that the NIPC did not obligate were "no-year" funds that remained available for fiscal year 2001. The NIPC used the funds to support its analysis and warning activities, investigation of computer crime, and outreach and information sharing with government and private-sector entities.

Most of the funding was reportedly used for activities performed by NIPC staff located at FBI headquarters in Washington, D.C. On the basis of the documents provided, the NIPC used about 16 percent of its fiscal years 1999 and 2000 funds to pay for training, travel, and information technology for NIPC field squads and teams located in FBI field offices. These funds were in addition to the salaries and expense amounts provided by the FBI field offices to the NIPC field squads and teams. According to FBI officials, the amounts reportedly used to support the NIPC field squads and teams by their respective FBI field offices could not be readily determined because those amounts are not accounted for separately from other FBI field operations. In addition, the salary amounts for the FBI agents and support staff assigned to the NIPC were estimated because the agents' salaries are not accounted for separately from other FBI operations.

The FBI Provided Funds to the NIPC on the Basis of Congressional Direction and NIPC Requirements

Justice appropriations laws for fiscal years 1999 and 2000 did not specify funding or provide specific direction for the NIPC; however, funding guidance was provided in congressional conference reports related to Justice's fiscal years 1999 and 2000 appropriations.[1] The sources and amounts specified in this funding guidance are identified in tables 4 and 5.

Table 4: Fiscal Year 1999 NIPC Funding Specified in Congressional Conference Report

Source of funding	Amount specified
FBI salaries and expenses	$33,542,000
Department of Justice Counterterrorism Fund	10,000,000
Department of Justice Working Capital Fund, if available, for an early warning system	4,250,000
Total	**$47,792,000**

The conference report earmarked $10.1 million from the fiscal year 1999 FBI salaries and expenses appropriation for the following purposes:

- $8.7 million for positions to establish four additional Computer Intrusion Threat Assessment field squads, which became NIPC field squads;
- $0.5 million for equipment for the new field squads;
- $0.4 million for additional positions for the NIPC's Watch and Warning Analysis Unit; and
- $0.5 million for training programs related to computer crime detection.

[1]House of Representatives, Conference Report 825, 105th Congress, Second Session 1998, *Making Omnibus Consolidated and Emergency Supplemental Appropriations of Fiscal Year 1999* and House of Representatives, Conference Report 479, 106th Congress, First Session 1999, *Making Appropriations for the Government of the District of Columbia and Other Activities Chargeable in Whole or in part Against Revenues of Said District for the Fiscal Year Ending September 30, 2000, and for Other Purposes*.

Table 5: Fiscal Year 2000 NIPC Funding Specified in Congressional Conference Report

Source of funding	Amounts specified
FBI salaries and expenses: National Infrastructure Protection Center/Computer Intrusion	$18,596,000
Estimated carryover available from fiscal years 1998 and 1999 no-year funds from the Violent Crime Reduction Trust Fund, the Department of Justice Counterterrorism Fund, and the Department of Justice Working Capital Fund	2,069,436
Total	**$20,665,436**

The fiscal year 2000 conference report noted that the new funding combined with the estimated carryover from fiscal years 1998 and 1999 would provide the NIPC with "approximately the same level of funding available in fiscal year 1999, adjusted for some nonrecurring requirements." According to FBI officials, the carryover discussed in the report was an estimated amount provided to congressional appropriations staff and was not meant to represent the final amount available because, at the time of congressional conferences, the fiscal year-end amount of carryover was not known. In addition, the conference report designated $1,250,000 from the fiscal year 2000 FBI salaries and expenses appropriation for the establishment of a "cybercrime" partnership with the Thayer School of Engineering at Dartmouth College.

On the basis of subsequent discussions with appropriations committee staffs,[2] the FBI ultimately provided funding to the NIPC that differed from the amounts specified in the conference reports. According to FBI Finance Division officials, the funding amounts agreed to and provided by the FBI were based on the NIPC's estimated requirements, as established in the President's budget requests. Tables 6 and 7 summarize the sources and amounts of NIPC funding for fiscal years 1999 and 2000. In fiscal year 1999, the FBI provided the NIPC with $15.9 million less than specified in the conference report and, in fiscal year 2000, $7.3 million more than specified in the conference report.

[2]According to FBI officials, discussions regarding fiscal years 1999 and 2000 NIPC funding were held with staff from the Subcommittee on Commerce, Justice, State and the Judiciary, Senate Committee on Appropriations, and the Subcommittee on Commerce, Justice, State and the Judiciary, House Committee on Appropriations.

Table 6: Fiscal Year 1999 Funding Provided to the NIPC From the FBI

Source of funds	Amounts available
Fiscal year 1999 funds	
Salaries and expenses	$9,435,000
No-year funds	
Violent Crime Reduction Trust Fund	5,900,000
Violent Crime Reduction Trust Fund carryover From fiscal year 1998	2,317,442
Department of Justice Counterterrorism Fund	10,000,000
Department of Justice Working Capital Fund	4,250,000
Total	**$31,902,442**

Table 7: Fiscal Year 2000 Funding Provided to the NIPC From the FBI

Source of funds	Amounts available
Fiscal year 2000 funds	
Salaries and expenses	$10,071,000
Estimated amount from Department of Justice reprogrammed and reallocated for a fiscal year 2000 FBI compensation and benefits shortfall[a]	771,968
No-year funds	
Violent Crime Reduction Trust Fund, including	
$1.25 million for Thayer School of Engineering	9,150,000
Fiscal year 1999 carryover	666,608
Fiscal year 1998 carryover	142,769
Department of Justice Counterterrorism Fund Carryover	5,272,023
Department of Justice Working Capital Fund Carryover	1,930,624
Total	**$28,004,992**

[a]According to FBI officials, the FBI received $68.4 million in reprogrammed and reallocated funds for fiscal year 2000 to meet a compensation and benefits shortfall.

In addition to the funding provided from the FBI, the NIPC received resources during fiscal years 1999 and 2000 in the form of administrative services from other FBI divisions and detailees from other government agencies. The FBI provided to the NIPC budgeting, accounting, training, telecommunications, and facilities services, which are typically provided to all FBI operational organizations, including the Counterterrorism Division, at no cost to the NIPC. For example, the FBI Finance Division provided support for NIPC's budget formulation and execution and maintained

accounting records, and the FBI's National Security Division provided requisition processing and document maintenance. Also, some of the training and related travel expenses for NIPC personnel were covered by the FBI's Quantico training facility without reimbursement. In addition, the Information Resources Division provided the NIPC with basic telecommunications services at no cost to the NIPC, but the NIPC had to pay for specialized telecommunications requirements, which are reflected in table 8. Further, the FBI provided the NIPC with the facilities occupied in the FBI building without reimbursement.

At least 39 detailees also served at the NIPC for varying periods. Although information regarding departure dates for some detailees was incomplete, at least 19 of the 39 people served for less than 12 months. All detailees were provided on a nonreimbursable basis.

Funds Primarily Used to Support The NIPC

On the basis of our analysis of documents provided by the NIPC and the FBI Finance Division, about 84 percent of the funds that the NIPC obligated in fiscal years 1999 and 2000 were for activities conducted at the NIPC in Washington, D.C. The NIPC used the rest of the funds it obligated to support the NIPC field squads and other NIPC teams located in FBI field offices. Table 8 details the amounts obligated for the NIPC in fiscal years 1999 and 2000. FBI Finance Division and NIPC officials developed all of the amounts shown on the basis of information extracted from FBI accounting records. Amounts for salaries, including compensation and benefits, were estimated because the FBI's accounting records did not segregate funds applicable to the FBI agents and support personnel assigned to the NIPC from other FBI obligations.

For fiscal years 1999 and 2000, combined, the NIPC obligated funds for the following key items:

- Salaries for FBI personnel assigned to the NIPC (32 agents and about 60 support personnel) ($14.9 million).
- Information technology, including hardware and software, for the NIPC ($7.1 million) and the field squads and teams ($4.8 million).
- Contracts ($12 million) that supported
  - a foreign counterintelligence investigation;
  - the NIPC's emergency law enforcement sector responsibilities, including providing case summaries and an emergency law enforcement services sector draft plan;
  - development of InfraGard Program information;

- development of periodic articles;
- development of training courses, exercises, and software tools;
- development of an incident analysis database;
- development of an early warning system that is intended to link numerous sources of electronic information to facilitate searches and accelerate investigations;
- research of existing and future Internet topology, including development of related tools to support investigations; and
- a "help desk" function for the NIPC.

- NIPC field squad training, including related travel, for Key Asset Initiative conferences, technical courses, and NIPC-related courses at the FBI's Quantico, VA, training facility ($3.3 million).

Table 8: Amounts Obligated by the NIPC During Fiscal Years 1999 and 2000

	Obligated amounts	
	FY 1999	**FY 2000**
Single-year funds obligated		
Salaries	**6,614,888**	**8,271,923**
Expenses		
Other tuition and training	48,426	36,789
Advisory and assistance	692,629	513,425
Routine travel	554,361	540,414
Regional conference travel	68,048	456,631
Miscellaneous other services	292,406	40,256
Routine supplies	84,813	79,976
NIPC equipment	751,700	325,554
Telecommunications	80,184	485,000
Conference room space rental	3,650	--
Confidential expenditure	150,000	93,000
Compensation and benefits (NIPC overtime)	35,800	--
Subtotal	**2,762,017**	**2,571,045**
Total	**9,376,905**	**10,842,968**
No-year funds obligated		
Violent crime reduction trust fund obligations		
Routine travel	78,039	51,548
Regional conference travel	358,018	59,914
Temporary duty travel	120,968	19,531

(Continued From Previous Page)

	Obligated amounts	
	FY 1999	**FY 2000**
Consulting services	1,611,355	4,453,427
Non-GSA building maintenance	1,300,000	--
Office equipment	1,765,012	3,550,429
Other automated data processing services	--	223,882
Commercial training	--	92,588
Other tuition/training services	--	60,000
Late payment penalty	--	25,771
Subtotal	**5,233,392**	**8,537,090**
Fiscal year 1998 carryover		
Routine travel	356,323	42,923
Regional conference travel	5,788	--
Temporary duty travel	57,397	--
Other tuition and training	123,468	--
Consulting services	187,596	--
Office equipment	1,365,820	99,846
Subtotal	**2,096,392**	**142,769**
Fiscal year 1999 carryover		
Routine travel	--	181,963
Regional conference travel	--	80,101
Temporary duty travel	--	27,982
Consulting services	--	18,029
Other automated data processing services	--	46,441
Office equipment	--	65,604
Subtotal	**--**	**420,120**
Total	**7,329,784**	**9,099,979**
Counterterrorism fund obligations		
Routine travel	--	3,241
Miscellaneous telecommunications	--	43,115
Other tuition and educational training	--	976,180
Consulting services	2,884,878	831,365
Non-GSA building maintenance	398,349	--
Miscellaneous services	380,886	--
Automated data processing services	621,088	--
Supplies	83,541	31,123
Intelligent workstations	--	53,975
Office equipment	358,500	2,966,012

(Continued From Previous Page)

	Obligated amounts	
	FY 1999	FY 2000
Late payment penalty	735	6,532
Total	**4,727,977**	**4,911,543**
Department of Justice working capital fund obligations		
Rental of miscellaneous equipment	10,022	--
Automated data processing services	1,414,055	682,522
Consulting services	185,560	1,221,670
Office equipment	708,141	21,977
Miscellaneous services	1	--
Late payment penalty	1,597	--
Total	**2,319,376**	**1,926,169**
Total no-year funds obligated	**14,377,137**	**15,937,691**
Total obligated amount for the NIPC	**23,754,042**	**26,780,659**

Conclusions

From the information provided by the NIPC and the FBI Finance Division, the FBI appears to be funding the NIPC on the basis of the congressional direction provided in the relevant conference reports and subsequent discussions with appropriations committee staffs. The NIPC used those funds primarily to support activities performed by NIPC staff located at FBI headquarters in Washington, D.C. About 16 percent of the NIPC's available funding was used to support the NIPC squads and teams at FBI field offices. We are making no recommendations regarding the NIPC's use of funds.

Agency Comments

In commenting on a draft of this report, the Director of the NIPC noted that our report stated that the FBI appears to be funding the NIPC on the basis of congressional direction. Neither the NIPC comments nor those of the Special Assistant to the President provided any additional references to this chapter.

Comments From the National Infrastructure Protection Center

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

April 4, 2001

Mr. Robert Dacey
Director
Information Security Issues
General Accounting Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Dacey:

Thank you for providing the Department of Justice (DOJ) and the National Infrastructure Protection Center (NIPC) with the opportunity to respond to the draft of the GAO's report entitled, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities." I am gratified that the report recognizes the effectiveness of the NIPC's internationally coordinated investigative program, the nationwide InfraGard program, and the NIPC's training program. Also the report found that "the FBI appears to be funding the NIPC based on...congressional direction." Your thorough report displays a commendable breadth and depth of knowledge concerning infrastructure protection issues and your efforts, together with the professional manner in which the GAO conducted this review, are most appreciated.

Although the majority of GAO's findings are positive, the NIPC considers it of the utmost urgency to address any shortcomings the GAO has identified. The NIPC is constantly maturing and, in that process, looks forward to achieving even greater success. Each accomplishment we have had to date, and every success to come, can only be achieved through a continual review and refinement of our operations. We intend to meet these challenges head-on.

Yet, without removing the barriers that the NIPC has faced in the past, it is unlikely that the NIPC can ever fully meet its own expectations, or those of Congress, the Executive Branch, and most importantly, the public. Therefore, with respect to those specific areas in which the NIPC's performance shows room for improvement, we find it constructive to emphasize the constraints under which the NIPC has operated and, in doing so, to emphasize how the elimination of those obstacles would dramatically

Mr. Robert Dacey

increase our capabilities, produce ever-greater results, and better serve our nation.

First and foremost, we highlight the GAO's recognition that the NIPC's ability to completely achieve its mission is most affected by a shortage of personnel resources. I must point out, in this regard, that despite these limitations, the dedicated men and women of the NIPC have done an outstanding job. I commend their commitment to public service and their oftentimes heroic and anonymous efforts on behalf of all Americans. Yet, without an increased staff, and one that is more representative of the diverse interests represented in the infrastructure protection community, the NIPC simply cannot reach its full capacity to assess, warn and protect.

I believe that the GAO report should reflect that many Executive Branch components simply have not heeded the call set out in Presidential Decision Directive 63 (PDD-63) to "provide such assistance, information and advice that the NIPC may request." While we are grateful to our partners in the Center who have provided assistance, it is nonetheless evident that the staffing resources provided from other Executive Branch components to the NIPC has been insufficient to allow the Center to more fully meet the enormous challenges of infrastructure protection.

In this regard, it is most important that the NIPC receive more adequate staffing, particularly from the defense and intelligence communities, in order to remedy the principal shortcoming identified by the GAO - the lack of strategic analysis. The NIPC was intentionally structured to assure the confidence of the defense and intelligence communities in the ability of the NIPC to disseminate timely intelligence material to their respective missions. The leadership of the Analysis and Warning Section, which is responsible for the production of strategic analysis, is reserved for a Central Intelligence Agency officer, and the managers of the units responsible for the production and sharing of analytic products are reserved for the National Security Agency and the military components of the Defense Department, respectively. To date, the intelligence and defense communities have only partially staffed these positions, oftentimes sporadically and never for lengthy periods that would offer consistency in management. Similarly, these communities have not assigned analytical support which is sufficient to fully accomplish the Center's mission. With more of a commitment from these and other Executive Branch agencies, the NIPC is well-positioned to provide more and better strategic analysis.

2

Mr. Robert Dacey

Second, we recommend that the GAO's report recognize the NIPC's performance in the context of its recent formation. The NIPC is not a longstanding entity. Rather, it is a start-up organization less than three years old which has accomplished admirable results despite the fact that it began with no dedicated source of funding and no ready group of personnel to staff it. Similarly, the political reality of any new government entity is that the NIPC operates in a milieu of federal agencies and for-profit entities that feel the NIPC threatens their resources or authorities. As such, the NIPC has had to overcome a rather high initial hurdle. Many of those upon whom the NIPC relies to accomplish its mission might prefer that the NIPC, especially as housed in the FBI, not succeed. Amidst this political environment, the NIPC has risen to the occasion of confronting the challenges of infrastructure protection, one of the most difficult and complex national security and public safety issues ever to face the U.S. government.

We therefore are proud to reiterate that, as the report points out, despite the formidable hurdles it has faced, the NIPC has in a short time achieved remarkable success. The NIPC created and managed a nationwide investigative program in 56 FBI field offices, in cooperation with the domestic and international law enforcement communities, that has proven its ability to successfully investigate extremely complicated and significant computer intrusion investigations. The NIPC developed and maintains effective working relationships with domestic and foreign law enforcement and security services, and it successfully created new and critical relationships with the private sector. These capabilities, in aggregate, did not exist anywhere in the United States before the creation of the NIPC.

The NIPC, as liaison for the Emergency Law Enforcement Sector (ELES) and in conjunction with the ELES Forum, is alone among all the sectors identified by PDD-63 to produce an infrastructure protection plan. The ELES Plan and an accompanying Guide was delivered to the National Coordinator on March 2, 2001, and presented as a model to the Partnership for Critical Infrastructure Security on March 20,2001.

The NIPC created a framework for sharing threat and vulnerability information between the federal government and private industry. This framework is critical to the government's ability to gather indications of a cyber attack and issue warnings in order to prevent or mitigate damage. The NIPC has created a solid foundation that has already proven beneficial to the government and private sector in our mutual efforts to address cyber threats.

3

Mr. Robert Dacey

Third, we would emphasize the significance of the fact that, despite certain political forces suggesting otherwise, GAO does not recommend a change to the basic PDD-63 framework. The initial justification for placing the NIPC within the FBI remains sound. It should be noted that the NIPC, under the authority of the FBI, is the only locus where law enforcement, counterintelligence, foreign intelligence, and private sector information may be lawfully and collectively 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 00-60, issued on March 8,2001 and December 1,2000, respectively, are examples of warnings which effectively combine law enforcement, intelligence and private sector information with the NIPC's warning mission, reflecting the balance of dissemination of information to the public with an ongoing law enforcement investigation, achieving both goals in the public's interest. It is also important to note that the Advisories 01-003 and 00-60 were coordinated in advance with private sector entities, including three separate Information Sharing and Analysis Centers (ISAC) and the Systems Administration and Networking Security Institute, reflecting the growing cooperative arrangement which exists between the NIPC and the private sector. One measure of the success of Advisory 01-003 is reflected in the statement by the Financial Services ISAC that the NIPC's advisory caused 1600 penetration attempts to be thwarted. These important advisories are a testament to the fact that analysis and warning not only is possible from an NIPC housed within the FBI, they reconfirm that the FBI is critical to the success of the NIPC's mission.

Fourth, in order to provide the most complete picture possible, the NIPC recommends that the GAO report highlight not only the positive interactions that the NIPC has had with much of the private sector, but also articulate the underlying causes that have led some others in the private sector to offer a limited, uneven record of cooperation with the government. To the extent the private sector has indicated a reluctance to share proprietary information with the government - a condition not unique to the NIPC - they have indicated a lack of understanding or perhaps confidence in the strength of the 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. In light of these concerns, the NIPC has reached out to communities across our nation to build trust and to educate the public on the legal and security aspects of information sharing and protection. The NIPC expanded a regional grassroots movement that promotes two-

Mr. Robert Dacey

way information sharing, called InfraGard, into a nationwide partnership which boasts 956 members at this writing, an increase of 84% from only 3 months ago. InfraGard, unlike some other Information Sharing and Analysis Centers which are operated by for-profit entities, is open - and free of charge - to all American businesses. The NIPC has also established a successful real-time information sharing relationship with the North American Electric Reliability Council (NERC), the electric power ISAC, and is in discussion with other sectors about replicating this model.

Of course, information sharing requires discipline and structure from all participants for it to be effective. Each principal component in infrastructure protection - industry, law enforcement, national security, system administration, and others - operates under internal and external constraints on information sharing. The reasons for such restrictions are based upon important considerations in each component's mission, including protection of sources and methods and protection of privacy. In order to build trust among these component groups, each group must be assured that shared information will be handled appropriately by the receiving entity. Therefore, DOJ and NIPC have worked, and will continue to work, to develop effective protocols that allow for maximum information sharing within the bounds of each component's legal and policy structures, and also provide a level of certainty that shared information will be appropriately protected. I believe that through such protocols, information necessary for protecting infrastructures can be timely and effectively shared.

In summary, we agree with the GAO that the fundamental factor affecting the performance of the NIPC is inadequate resources. As such, the NIPC's improving performance and significant successes are all the more remarkable given its start from "scratch" less than three years ago, the politically challenging environment in which it operates, its lack of a dedicated funding stream, and misperceptions in the private sector about the government's ability and commitment to protect proprietary information. The GAO's recognition of the effectiveness of the NIPC's investigative, InfraGard and training programs reflects this progress. At the same time, the NIPC recognizes its need to do better and is working diligently to improve. The GAO report is welcomed as a yardstick to measure the NIPC's improvement and as a means to prioritize its limited resources.

5

Mr. Robert Dacey

Again, thank you for the opportunity to review and comment on the draft report. If you have any questions or desire additional discussion, please contact me.

Sincerely,

Ronald L. Dick
Director
National Infrastructure
Protection Center

6

Comments From the National Security Council

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

April 9, 2001

Dear Mr. Dacey:

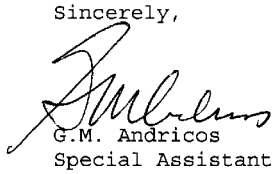
On behalf of the National Security Advisor, thank you for the opportunity to comment on your draft report entitled Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. The report's findings on the progress of the National Infrastructure Protection Center (NIPC) in addressing cyber threats to national infrastructures highlight the need for a review of the roles and responsibilities of federal agencies involved in U.S. critical infrastructure protection (CIP) support. As noted in your report, the NIPC has been successful in providing CIP support to law enforcement, due in part to their close proximity to FBI headquarters and working relationships with FBI field offices. NIPC has not been as successful in some of their other CIP initiatives.

We are currently reviewing federal cyber activities in the broader context of determining how the federal CIP functions should be organized. Some CIP functions might be better accomplished by distributing the tasks across several existing federal agencies, creating a 'virtual analysis center' that would provide not only a government-wide analysis and reporting capability, but could also support rapid dissemination of cyber threat and warning information. Other functions could be shifted to federal agencies that do not have the policy and legal impediments that are inherent in the NIPC.

The recommendations in your report will be considered as we assess the requirements to provide comprehensive protection of U.S. critical infrastructures. We are confident that the outcome will ultimately improve the nation's ability to respond

to cyber threats, share information, and protect our critical infrastructures.

Sincerely,



G.M. Andricos
Special Assistant to the President
and Senior Director for
Legislative Affairs

Mr. Robert F. Dacey
Director, Information Security Issues
United States General Accounting Office
Washington, DC 20548

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00