United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

July 2002

CRITICAL INFRASTRUCTURE PROTECTION

Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems

G A O

Accountability ★ Integrity ★ Reliability

GAO-02-474

GAO
Accountability★Integrity★Reliability

Highlights

CRITICAL INFRASTRUCTURE PROTECTION Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems

Highlights of GAO-02-474, a report to the Committee on Governmental Affairs, U.S. Senate.

Why GAO Did This Study

The explosion in computer interconnectivity, while providing great benefits, also poses enormous risks. Terrorists or hostile foreign states could launch computer-based attacks on critical systems to severely damage or disrupt national defense or other critical operations.

Presidential Decision Directive 63 and Executive Order 13231, issued in 1998 and 2001, respectively, call for various actions to improve federal security programs, including establishing partnerships between the government and the private sector. GAO was asked to identify the federal organizations that have national roles for protecting critical infrastructures from computer-based attacks and to determine their relationships.

What GAO Recommends

GAO recommends that when developing the strategy to guide federal CIP efforts, senior executive branch officials ensure that, among other things, it includes all relevant sectors, defines the key federal agencies' roles and responsibilities associated with each sector, and defines the relationships among the key CIP organizations.

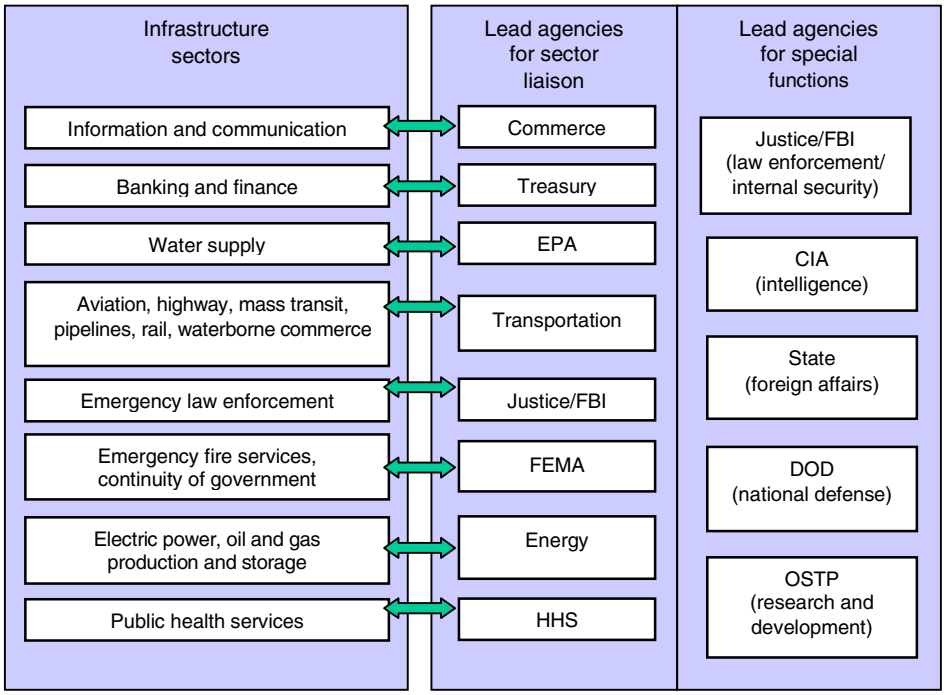
In commenting on a draft of this report, the agencies primarily provided technical comments, which were included in the report, as appropriate.

What GAO Found

GAO identified at least 50 federal organizations that have various national or multiagency responsibilities related to cyber critical infrastructure protection (CIP), several of which are shown in the figure below. However, current cyber CIP efforts do not specifically address all critical infrastructure sectors or federal agencies. For example, Directive 63 excludes key infrastructure sectors and their respective federal agencies associated with chemical manufacturing and food safety. According to the chair of the President's Critical Infrastructure Protection Board, the infrastructures originally identified in PDD 63 are now being reevaluated in view of the events of September 11, 2001.

Although most organizations could identify their relationships with other key cyber CIP entities, relationships among all organizations performing similar activities (e.g., incident response or research and development) were not consistently established. The President's Critical Infrastructure Protection Board, created under Executive Order 13231, is intended to coordinate federal efforts and programs related to protecting critical infrastructures. However, an underlying challenge in this coordination is that a detailed strategy is being developed. Without a strategy that identifies responsibilities and relationships for all cyber CIP efforts, our nation risks not having the appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructures.

Several Key Organizations with CIP Responsibilities as Outlined by PDD 63.



This is a test for developing Highlights for a GAO report. The full report, including GAO's objectives, scope, methodology, and analysis is available at www.gao.gov/cgi-bin/getrpt?GAO-02-474. For additional information about the report, contact Robert F. Dacey (202-512-3317). To provide comments on this test Highlights, contact Keith Fultz (202-512-3200) or e-mail HighlightsTest@gao.gov.

Contents

Letter

	1
Results in Brief	2
Background	4
At Least 50 Federal Organizations Derive Their Cyber CIP Responsibilities from a Variety of Sources	14
Relationships among Cyber CIP Organizations Are Not Consistently Established	23
CIP Funds Are Not Separately Appropriated for Most Organizations, and Precise Levels of Spending Cannot Be Ascertained	26
Conclusions	28
Recommendation	28
Agency Comments and Our Evaluation	29

Appendixes

Appendix I:	**Objectives, Scope, and Methodology**	32
Appendix II:	**Federal Organizations Involved in National or Multiagency Cyber CIP Efforts**	34
	Federal Advisory Committees	34
	Executive Office of the President	36
	Chief Information Officers Council	40
	National Communications System	40
	Federal Communications Commission	41
	U.S. Department of Commerce	42
	U.S. Department of Defense	45
	Director of Central Intelligence	50
	U.S. Department of Energy	52
	U.S. Department of Justice	54
	U.S. Department of Transportation	56
	Environmental Protection Agency	57
	Federal Emergency Management Agency	57
	U.S. General Services Administration	59
	Department of Health and Human Services	60
	National Science Foundation	61
	U.S. Department of State	62
	U.S. Department of the Treasury	64

Appendix III: Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP 66

Appendix IV: Comments from the Department of Justice 69

Appendix V: Comments from the Special Advisor to the President for Cyberspace Security 70

Appendix VI: Comments from the Office of Science and Technology Policy 71

Appendix VII: Comments from the Federal Emergency Management Agency 73

Appendix VIII: Comments from the Department of State 74

Appendix IX: GAO Contact and Staff Acknowledgments 77

GAO Contact 77

Acknowledgments 77

Tables

Table 1: Observed Threats to Critical Infrastructure 5

Table 2: Key Executive Orders, Presidential Decision Directives, Acts, and Directives That Mention Activities Related to Cyber CIP 20

Table 3: Office of Homeland Security Fiscal Year 2002 and 2003 CIP Funding 27

Table 4: Executive Department or Agency Components and Their Primary Activities Related to Cyber CIP 66

Figures

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT®, Coordination Center: 1990–2001 6

Figure 2: Organizations with CIP Responsibilities as Outlined by PDD 63 10

Figure 3: Overview of National or Multiagency Federal Cyber CIP Organizations 16

Figure 4: Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as indicated by the Color-Coded Legend Below) 17

Abbreviations

CIAO	Critical Infrastructure Assurance Office
CIP	critical infrastructure protection
DOD	Department of Defense
ECIE	Executive Council on Integrity and Efficiency
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
GSA	General Services Administration
ISAC	information sharing and analysis center
NIAC	National Infrastructure Assurance Council
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCIE	President's Council on Integrity and Efficiency
PDD	Presidential Decision Directive
R&D	research and development
TSA	Transportation Security Administration

G A O
Accountability * Integrity * Reliability

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

July 15, 2002

The Honorable Joseph I. Lieberman
Chairman
The Honorable Robert F. Bennett
Committee on Governmental Affairs
United States Senate

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. 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, law enforcement, and critical government services. Because potential adversaries—be they nation-states, cyber terrorist groups, criminal organizations, or disgruntled insiders—can develop cyber-attack capabilities to attempt to exploit these risks, it is essential that our critical infrastructures be adequately protected.

Concerns about computer-based vulnerabilities have been reported repeatedly during the 1990s. Since 1997—most recently in January 2001—we, in reports to the Congress,[1] have designated information security 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.

In May 1998, Presidential Decision Directive 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. Critical infrastructure protection (CIP) involves activities that

[1]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update*, GAO/HR-99-1 (Washington, D.C.: January 1999); *High-Risk Series: An Update*, GAO-01-263 (Washington, D.C.: January. 2001).

[2]President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: October 1997).

enhance the security of our nation's cyber and physical public and private infrastructures that are essential to national security, national economic security, and/or national public health and safety. On October 16, 2001, President Bush issued Executive Order 13231, "Critical Infrastructure Protection in the Information Age," which continues many Presidential Decision Directive 63 activities by focusing on cyberthreats to critical infrastructures, and also created the President's Critical Infrastructure Protection Board to coordinate federal cybersecurity efforts.

In response to your request, we reviewed federal organizations involved in national or multiagency cyber CIP activities. Specifically, our objectives were to (1) identify the federal civilian, defense, and intelligence organizations involved in protecting critical infrastructures from computer-based attacks, and their responsibilities, current organizational placement, and source of authority; (2) identify the organizations' relationships with each other; and (3) determine appropriated CIP funds for each organization. As agreed with your staff, we concentrated on federal organizations identified in Presidential Decision Directive 63 or Executive Order 13231 that have a national or multiagency cyber CIP focus and did not address organizations involved solely in CIP activities specific to their department or agency, such as the agencies' critical infrastructure assurance offices. For example, although organizations such as the Federal Aviation Administration, the Centers for Disease Control, the Financial Management Service, and the National Weather Service are responsible for the security of critical cyber systems, they do not have national cyber CIP responsibilities outside their agencies. In addition, other information security organizations that receive federal funding were not included in our review. Further details on our objectives, scope, and methodology are provided in appendix I.

Results in Brief

At least 50 federal organizations are involved in national or multiagency cyber CIP activities that include setting policy, analyzing vulnerabilities and intelligence information, disseminating alerts and warnings on potential and actual infrastructure attacks, developing remediation plans, responding to incidents, and performing research and development. These organizations are primarily located within 13 major departments and agencies mentioned in Presidential Decision Directive 63. In addition to most of these organizations' noting that Directive 63 and Executive Order 13231 were the primary sources dictating their current cyber CIP roles and responsibilities, many identified other preexisting laws, directives, and orders that levy related requirements. Nevertheless, current cyber CIP

efforts do not specifically address all potentially relevant critical infrastructure sectors or federal agencies. For example, Directive 63 excludes some key infrastructure areas and their respective federal agencies, such as those associated with chemical manufacturing and food safety. The chair of the President's Critical Infrastructure Protection Board, as well as officials from the Critical Infrastructure Assurance Office, acknowledged that our nation's critical infrastructures are currently being redefined and could be expanded in view of the events of September 11, 2001. Such an effort is critical to ensuring that we are comprehensively addressing our nation's critical infrastructures.

Although most organizations could identify their relationships with other key cyber CIP entities, relationships among all organizations performing similar activities (e.g., policy development or analysis and warning) were not consistently established. The President's Critical Infrastructure Protection Board is intended to coordinate federal efforts and programs related to protecting critical infrastructures. However, an underlying challenge in this coordination is that a detailed strategy is still being developed. Without a strategy that identifies responsibilities and relationships for all cyber CIP efforts, our nation risks not knowing whether we have the appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure. The President's Critical Infrastructure Protection Board is currently developing a proposed national strategy in coordination with the private sector. It is essential that this strategy define the roles, responsibilities, and relationships among the various federal organizations involved in cyber CIP activities.

Most of the organizations in our review do not receive appropriations specifically designated for cyber CIP and, therefore, do not have a process to track these funds. A complicating factor in tracking funds spent on cyber CIP activities is that organizational totals often include funds spent on physical, cyber, and agency-specific CIP spending. A few selected organizations can readily identify their CIP funding since the majority, and in some cases all, of their operations are related to such activities. Overall, on the basis of agency input submitted to the Office of Management and Budget (OMB), the executive branch estimated that $3.9 billion was requested for CIP for fiscal year 2003. However, this total involves both physical and cyber CIP, and detailed breakdowns of these funds are not available. OMB plans to provide a more detailed breakdown in the future.

We are recommending that when developing the strategy to guide federal cyber CIP efforts, senior executive branch officials ensure that the strategy,

among other things, includes all relevant sectors, defines the key federal agencies' roles and responsibilities associated with each of these sectors, and defines the relationships among the key cyber CIP organizations.

In providing written comments on a draft of this report, the Department of Justice generally concurred with our findings and recommendations; the Special Advisor to the President for Cyberspace Security and the Department of State did not indicate whether they agreed or disagreed; the Federal Emergency Management Agency requested that we add an additional organization, and the Office of Science and Technology Policy (OSTP) disagreed with our statement that none of the R&D organizations coordinated with them. Specifically, on the basis of additional information the Federal Emergency Management Agency provided in an attachment, we added the Office of the Chief Information Officer and Information Technology Services Directorate and also incorporated additional technical comments, as appropriate. OSTP stated that it is inaccurate for us to imply that consultations are not occurring with the agencies with research and development (R&D); however, when we asked the R&D organizations who they coordinate with, none indicated that they coordinated with OSTP, nor did any of these organizations comment on this statement in our draft report that OSTP took exception to. We also received oral comments from nine agencies that have been incorporated into the report, as appropriate. Although the written and oral comments varied in scope and detail, they were primarily limited to technical comments on the description of their responsibilities described in appendix II. We have incorporated these changes in the report as appropriate. The Department of Transportation had no comments, and we did not receive comments from the Department of Commerce.

Background

The risks associated with our nation's reliance on interconnected computer systems are substantial and varied. 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 (NSA), 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. The threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups such as al Qaeda have used the Internet to launch a known assault on the U.S.'s infrastructure, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan. Table 1 summarizes the key threats to our critical infrastructures.

Table 1: Observed Threats to Critical Infrastructure

Threat	Description
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 hacking 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.
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,[a] 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 a victim system 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, the CIH (Chernobyl), and Nimda viruses and the Explore.Zip and CodeRed worms.

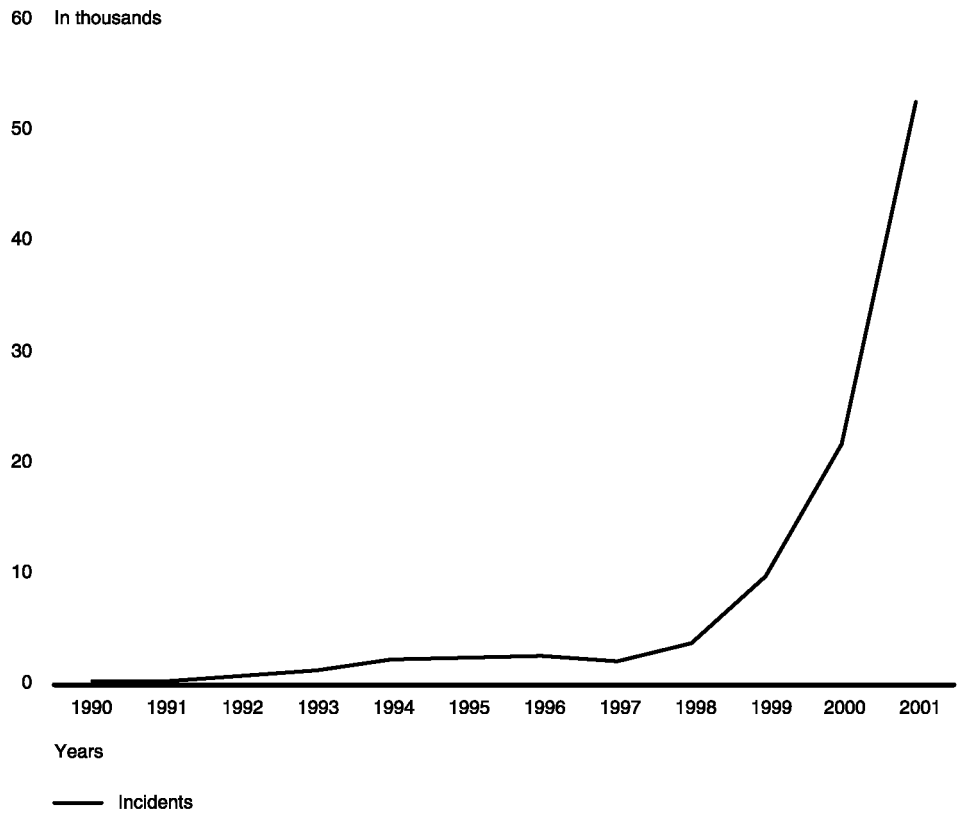
[a]Prepared Statement of George J. Tenet, director of central intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Source: Federal Bureau of Investigation.

The number of reported cyber-based incidents is increasing. Complete summary data are not available because many incidents are not reported. Nevertheless, the number of reported incidents handled by the

Carnegie-Mellon University CERT®, Coordination Center[3] continues to increase dramatically. For example, the number of incidents reported to the CERT®, Coordination Center during the first quarter of 2002 is more than half the number of incidents reported for all of 2001. Figure 1 shows the number of incidents reported to the CERT®, Coordination Center from 1990 through 2001.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center: 1990–2001



Source: Carnegie-Mellon's CERT® Coordination Center.

[3]The CERT® Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

The events of September 11, 2001, underscore the need to protect America's critical infrastructures against potentially disastrous cyberattacks—attacks that could also be coordinated to coincide with physical terrorist attacks to maximize the impact of both.

Critical Infrastructure Protection Policy Has Been Evolving Since the Mid-1990's

Federal awareness of the importance of securing our nation's cyber critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990's. Over the years, a variety of working groups have been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. 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 options for a full-time group to consider long-term government response to threats to critical infrastructures. The working group recommended creating a commission to further investigate the issues. In response to this recommendation, the President's Commission on Critical Infrastructure Protection was established in July 1996 to study the nation's vulnerabilities to both cyber and physical threats.

In October 1997, the President's Commission issued its report, which described the potentially devastating implications of poor information security from a national perspective. The report recommended several measures to achieve a higher level of critical infrastructure protection, including infrastructure protection through industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection. 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 cyberthreats." 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.

The President subsequently issued Presidential Decision Directive (PDD) 63, in 1998, which describes a strategy for cooperative efforts by

government and the private sector to protect critical, computer-dependent operations. PDD 63 called for a range of actions intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated lead agencies to work with private-sector and government organizations. Further, it established critical infrastructure protection as a national goal, and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, no later than 2003, an enhanced capability.

To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;

- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and

- the National Infrastructure Assurance Council (NIAC), which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.[4]

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. The infrastructures are (1) information and communications; (2) banking and finance; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. The special functions are (1) law enforcement and internal security, (2) intelligence, (3)

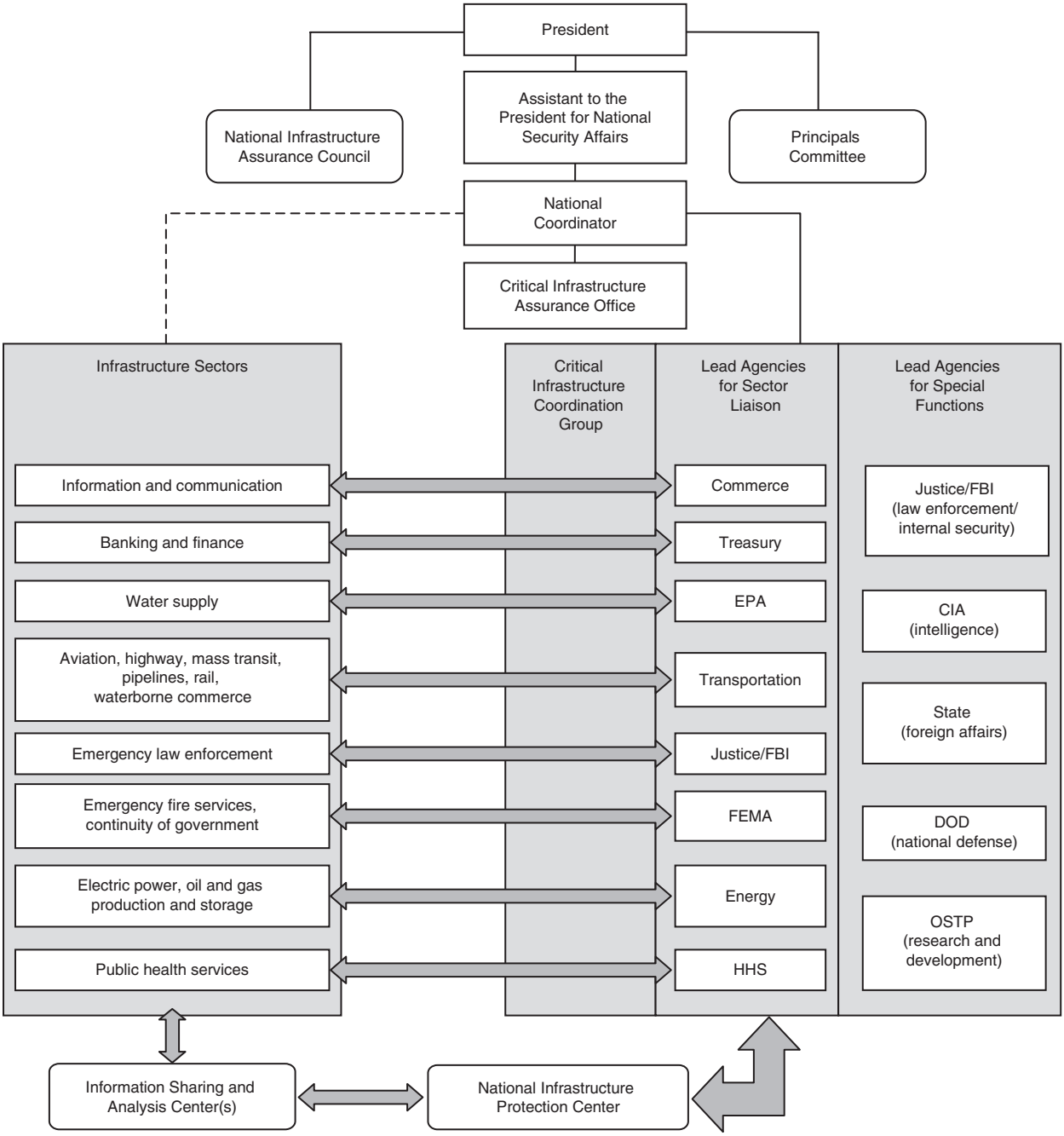
[4]Executive Order 13231 replaces this council with the National Infrastructure Advisory Council.

foreign affairs, (4) national defense, and (5) research and development. For each of the infrastuctures and functions, the directive designated lead federal agencies to work with their counterparts in the private-sector. 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 electrical 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 also encouraged the 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 federal government through the NIPC. In September 2001, we reported that six ISACs within five infrastructures had been established to gather and share information about vulnerabilities, attempted intrusions, and attacks within their respective infrastructures and to meet specific sector objectives.[5] Three of the ISACs—for the telecommunications and electric power industries and emergency fire services segment—were based on groups that had existed previously. The other three—for the financial services, information technology, and emergency law enforcement sectors—had been established since October 1999. In addition, at that time, we reported that the formation of at least three more ISACs for various infrastructure sectors were being discussed. Figure 2 displays a high-level overview of the organizations with CIP responsibilities as outlined by PDD 63.

[5]U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

Figure 2: Organizations with CIP Responsibilities as Outlined by PDD 63



Note: In February 2001, the Critical Infrastructure Coordination Group was replaced with the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee

on Counter-terrorism and National Preparedness. In October 2001, the National Infrastructure Assurance Council was replaced with the National Infrastructure Advisory Council, and cyber CIP functions performed by the national coordinator were assigned to the chair of the President's Critical Infrastructure Protection Board.

Source: CIAO.

In response to PDD 63, in January 2000 the White House issued its "National Plan for Information Systems Protection."[6] The national plan provided a vision and framework for the federal government to prevent, detect, respond to, and protect the nation's critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements. Subsequent versions of the plan were expected to (1) define the roles of industry and state and local governments working in partnership with the federal government to protect privately owned physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

The most recent federal cyber CIP guidance was issued in October 2001, when President Bush signed Executive Order 13231, establishing the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures. The Special Advisor to the President for Cyberspace Security chairs the board. Executive Order 13231 tasks the board with recommending policies and coordinating programs for protecting CIP-related information systems. The executive order also established 10 standing committees to support the board's work on a wide range of critical information infrastructure efforts. The board is intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications that were assigned to the Office of Homeland Security by Executive Order 13228, dated October 8, 2001. The board recommends policies and coordinates programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. In addition, the chair coordinates with the Assistant to the President for Economic Policy on issues relating to private-sector systems and economic effects and with the

[6]The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* (Washington, D.C.: 2000).

Director of OMB on issues relating to budgets and the security of federal computer systems.

Effective Federal Information Security Programs Are Critical to CIP

At the federal level, cyber CIP activities are a component, perhaps the most critical, of a federal department or agency's overall information security program. Since September 1996, we have reported that poor information security is a widespread federal government problem with potentially devastating consequences.[7] These information security programs include efforts to protect critical cyber assets owned by the federal government. Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in 1998, 2000, and 2002, we analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[8] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[9]

[7]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices.*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

[8]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

[9]GAO/HR-97-9, Feb. 1,1997; GAO-01-263, January 2001.

In March of this year, when we testified on the efforts by the federal government to implement provisions for Government Information Security Reform Act that were enacted as part of the National Defense Authorization Act for Fiscal Year 2001,[10] we highlighted the fact that each agencywide information security program is required to ensure the integrity, confidentiality, and availability of systems and data supporting the agency's critical operations and assets (e.g., CIP assets).[11] At that time, of 24 of the largest agencies, 15 had not implemented an effective methodology to identify their critical assets,[12] and 7 had not determined the priority for restoring these assets should a disruption in critical operations occur. OMB indicated that it was to direct all agencies to identify and prioritize their critical assets.

Our testimony was consistent with what the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) reported last year on the federal government's compliance with PDD 63. It concluded that the federal government could improve its planning and assessment activities for cyber-based critical infrastructures. Specifically, the council stated that (1) many agency infrastructure plans were incomplete; (2) most agencies had not identified their mission-critical infrastructure assets; and (3) few agencies had completed vulnerability assessments of mission-critical assets or developed remediation plans.

[10]*Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L. 106-398 (Oct. 30, 2000).

[11]GAO-02-470T, Mar. 6, 2002.

[12]The Department of Commerce's CIAO established Project Matrix to provide a standard methodology for identifying all assets, nodes, networks, and associated infrastructure dependencies and interdependencies required for the federal government to fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people.

At Least 50 Federal Organizations Derive Their Cyber CIP Responsibilities from a Variety of Sources

At least 50 organizations are involved in national or multiagency cyber CIP efforts and derive their responsibilities from PDD 63 and Executive Order 13231, as well as various other federal laws, directives, and orders. These organizations are involved in many cyber CIP activities, including policy development, vulnerability assessment, and research and development. However, current cyber CIP efforts do not specifically address all potentially relevant sectors and their respective federal agencies. The chair of the President's Critical Infrastructure Protection Board, as well as officials from the CIAO, acknowledged that our nation's critical infrastructures are currently being reexamined and could be expanded.

Many Organizations Have National or Multiagency Cyber CIP Responsibility

Protecting the nation's critical infrastructure against information attacks is a complicated process involving many organizations within many government agencies. At least 50 organizations are involved in national or multiagency cyber CIP efforts. These entities include 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations. These organizations are primarily located within 13 major departments and agencies mentioned in PDD 63.[13] Several departments, including DOD, Treasury, and Commerce have multiple organizations involved in cyber CIP activities. For example, we identified 7 organizations within DOD involved in national or multiagency cyber CIP efforts. Appendix II identifies each of the organizations, provides a high-level description of their cyber CIP responsibilities, and identifies their source(s) of authority.

Although each organization described a wide range of cyber CIP-related activities, collectively they described activities related to the following five categories:

- policy development, including advising on policy issues, coordinating and planning CIP activities, issuing standards and best practices, providing input to the national CIP plan, developing education and

[13]These are the Departments of Commerce, Defense, Energy, Justice, Transportation, Health and Human Services, State, and Treasury; and the Environmental Protection Agency, the Federal Emergency Management Agency, the General Services Administration, and the National Science Foundation.

outreach programs with governmental and private sector organizations, and coordinating internationally;

- analysis and warning, including conducting vulnerability analyses, gathering intelligence information, coordinating and directing activities to detect computer-based attacks, disseminating information to alert organizations of potential and actual infrastructure attacks, and facilitating the sharing of security-related information;

- compliance, including overseeing implementation of cyber CIP programs, ensuring that policy is adhered to and remedial plans are developed, and investigating cyberattacks on critical infrastructures;

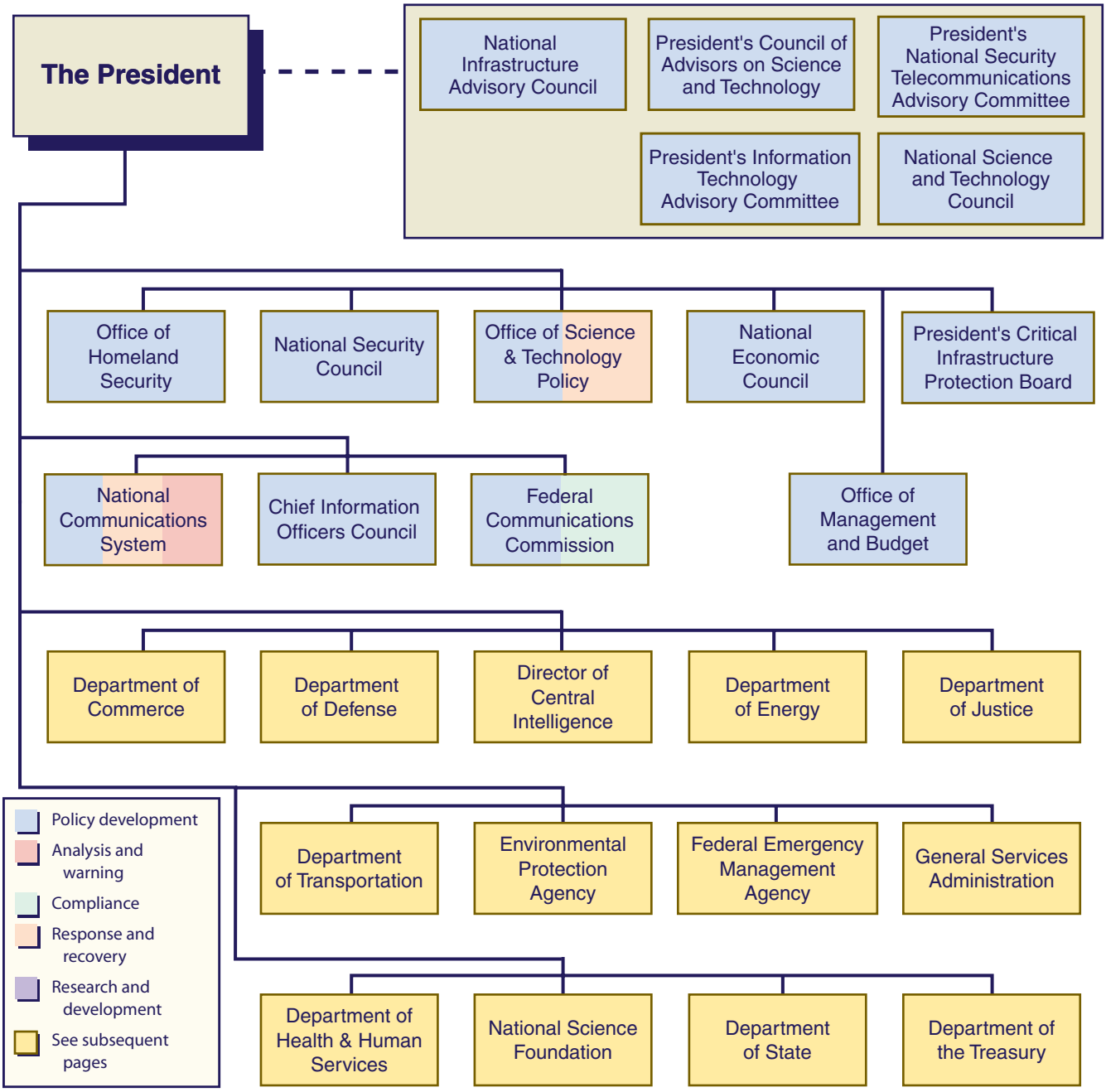
- response and recovery, including reconstituting minimum required capabilities, isolating and minimizing damage, and coordinating the necessary actions to restore functionality; and

- research and development, including coordinating federally sponsored research and development in support of infrastructure protection.

On the following page, figure 3 displays a high-level overview of the organizational placement of the 5 advisory committees; 6 Executive Office of the President organizations; 13 executive branch departments and agencies; and several other organizations involved in national or multiagency cyber CIP efforts. For departments and agencies, figure 4 provides further detail on component organizations' involvement, but does not illustrate the internal relationships within each agency. For all figures, organizations' cyber CIP-related activities are identified in one or more of the five general categories discussed above. Appendix III displays in tabular format the entities and their activities.[14]

[14]Figure 4 displays the five general CIP activities according to a color-coded legend. Appendix III provides an alternative (table format) for black and white printing.

Figure 3: Overview of National or Multiagency Federal Cyber CIP Organizations



Note: Major agencies or departments are highlighted in yellow here and in figure 4. The organizations are color-coded to correspond to one or more of the five general activities related to cyber CIP (see legend).

Figure 4: Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as indicated by the Color-Coded Legend Below)

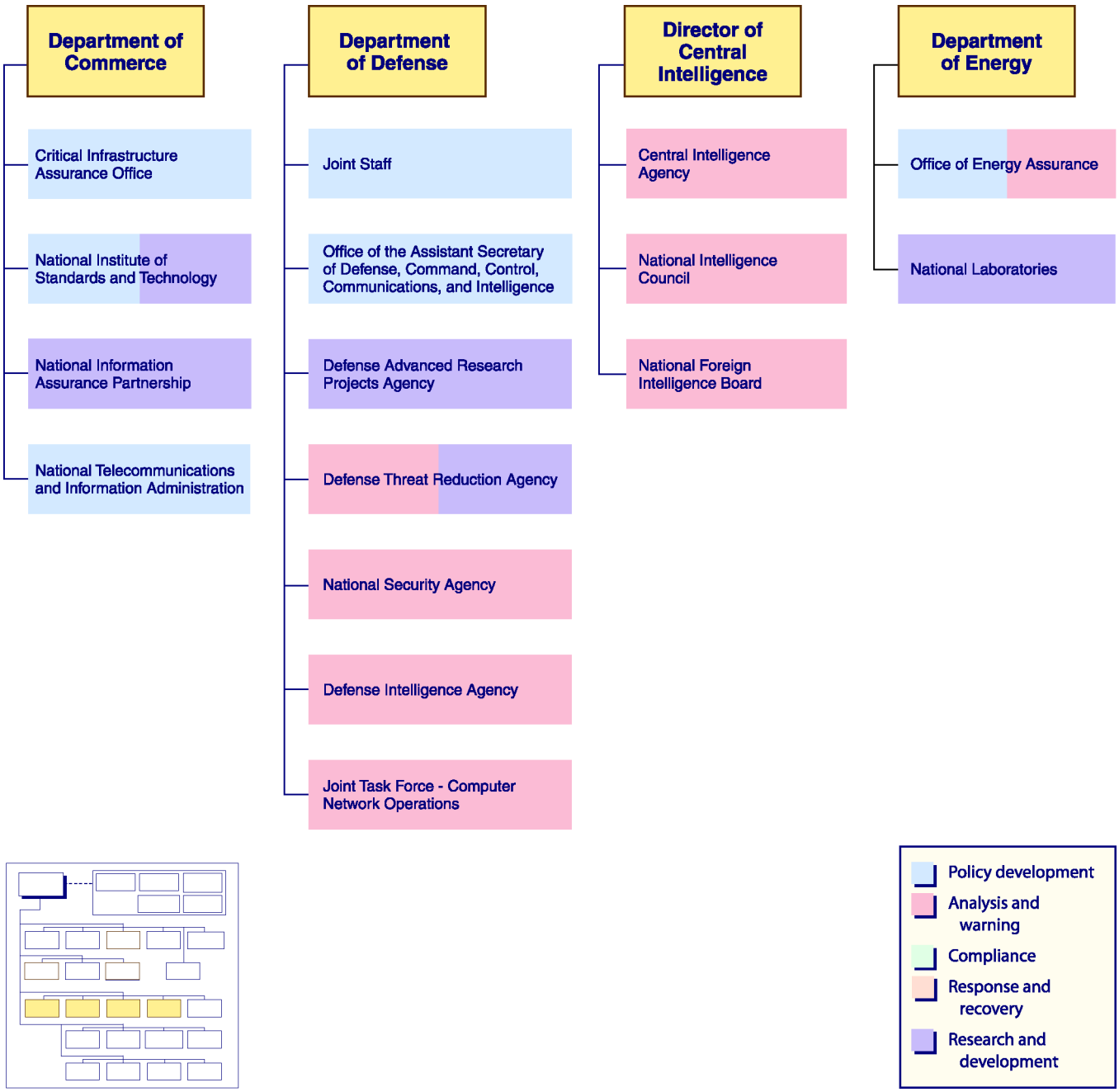


Figure 4 (cont'd): Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as Indicated by the Color-Coded Legend Below)

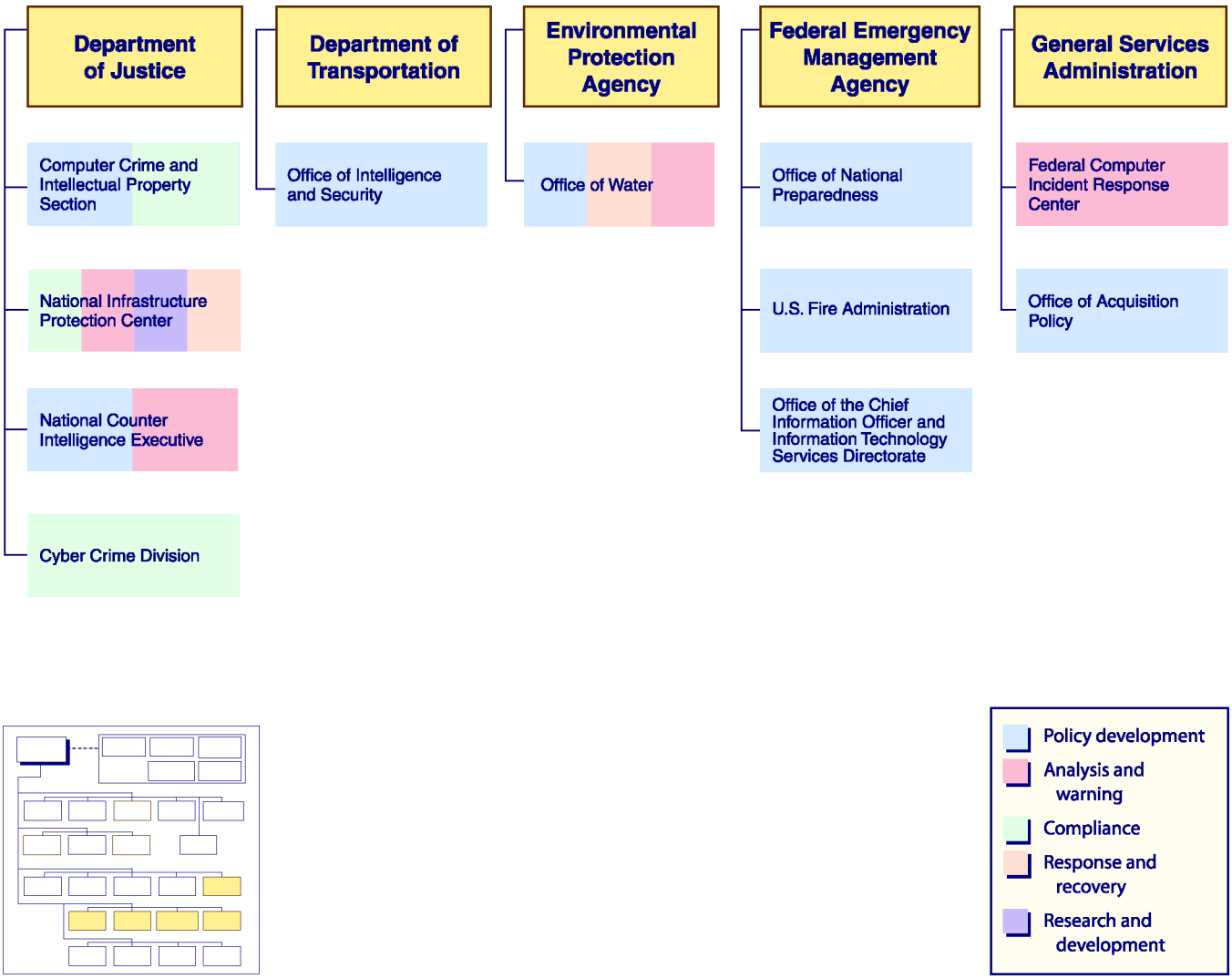
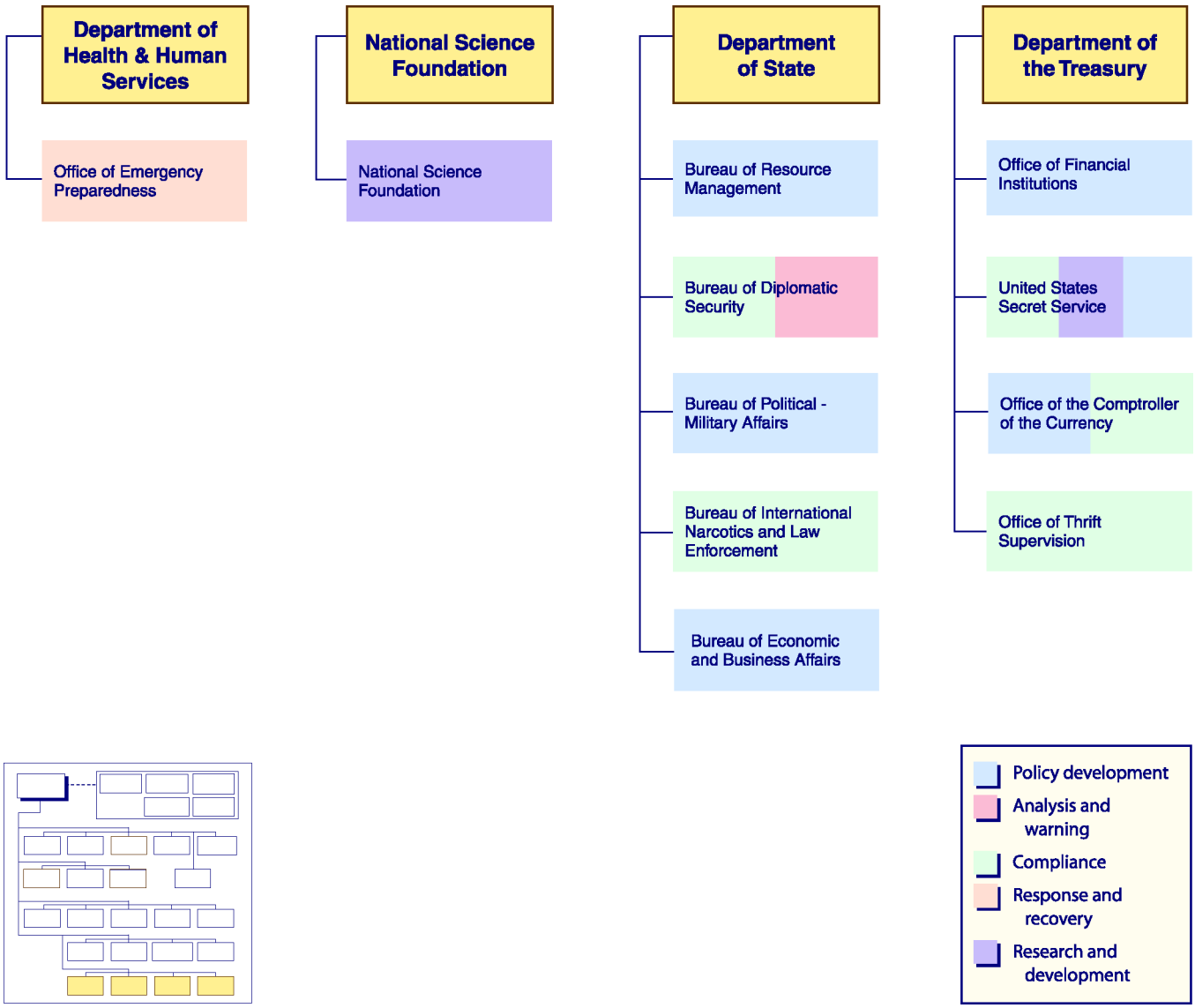


Figure 4 (cont'd): Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as Indicated by the Color-Coded Legend Below)



The President's recent proposal to create a cabinet-level Department of Homeland Security states that "currently, at least twelve different government entities oversee the protection of our critical infrastructure." As our analysis shows, at least 50 organizations are involved in national cyber CIP efforts.

Federal Organizations Derive Their Cyber CIP Responsibilities from a Variety of Laws, Regulations, and Federal Policy Documents

In addition to PDD 63 and Executive Order 13231, agencies derive and justify their cyber CIP efforts from a variety of laws, regulations, and federal policy documents. Various laws and regulations also address the need to secure federal systems, including the Government Information Security Reform Act; the Clinger-Cohen Act; the Computer Security Act; and Appendix III to OMB Circular A-130, *Security of Federal Automated Information Resources*. In addition to the overarching legislation mentioned above, table 2 below summarizes the key executive orders, presidential decision directives, and other acts and directives that mention activities related to cyber CIP.

Table 2: Key Executive Orders, Presidential Decision Directives, Acts, and Directives That Mention Activities Related to Cyber CIP

Law or regulation	Description
Executive orders	
Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions"	Signed in 1984, this order established the National Communication Systems and assigns national security emergency preparedness responsibilities for telecommunications.
Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities"	Signed in 1988, this order assigns federal national security emergency preparedness responsibilities to federal departments and agencies for various sectors.
Executive Order 13231, "Critical Infrastructure Protection in the Information Age"	Signed in October 2001, this order establishes the President's Critical Infrastructure Protection Board to coordinate the federal efforts and programs associated with protecting our nation's critical infrastructures. A special advisor to the President for cyberspace security chairs the board. This order also tasks the board to recommend policies and coordinate programs for protecting information systems for critical infrastructure protection. The executive order also established 10 standing committees to support the board's work on a wide range of critical information infrastructure efforts.
Executive Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council"	Signed in October 2001, this order establishes the Office of Homeland Security, whose mission is to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The office will coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

(Continued From Previous Page)

Law or regulation	Description
Presidential decision directives	
PDD 39, "Presidential Decision Directive on Terrorism"	Signed in 1995, this directive sets forth the U.S. general policy to use all appropriate means to deter, defeat, and respond to all terrorist attacks against U.S. interests. More specifically, PDD 39 directs federal departments to take various measures to (1) reduce the vulnerabilities to terrorism, (2) deter and respond to terrorism, and (3) develop effective capabilities to prevent and manage the consequences of terrorist use of weapons of mass destruction. The directive charges the FBI as the lead investigative agency to reduce U.S. vulnerabilities to terrorism.
PDD 62 "Combating Terrorism"	Signed in 1998, this directive established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. PDD 62 also reinforces the mission of many of the agencies charged with roles in defending terrorism by codifying and clarifying their activities in the range of counter-terrorism programs including the protection of the computer-based systems that support critical infrastructure sectors.
PDD 63, "Protecting America's Critical Infrastructures"	Signed in 1998, this directive expanded the NIPC at the FBI, and established ISACs in cooperation with the federal government, private sector, and the CIAO to support work in developing a national plan.
PDD 67, "Enduring Constitutional Government and Continuity of Government Operations"	Signed in 1998, this directive required federal agencies to develop continuity of operations plans for essential operations.
PDD 75, "U.S. Counterintelligence Effectiveness – Counterintelligence for the 21st Century"	Signed in 2001, this directive establishes a counterintelligence board of directors, the National Security Council Deputies Committee, and a National Counterintelligence Executive.
Other directive/acts	
National Security Directive 42, National Policy for the Security of National Security Systems	Signed in 1990, this directive designates the Director, NSA the national manager for national security telecommunications and information systems security and calls upon him or her to promote and coordinate defense efforts against threats to national security systems.
The Stafford Act	Enacted in 1974, this act enables the Federal Emergency Management Agency (FEMA) to provide supplementary federal assistance to individuals, state and local governments, and certain private nonprofit organizations to assist them in recovering from the devastating effects of major disasters.
The USA PATRIOT Act	Enacted in 2001, this act enables law enforcement entities to apply modern surveillance capabilities to new technologies, such as the Internet, and execute these devices in multiple jurisdictions anywhere in the United States.
The Aviation and Transportation Security Act	Enacted in 2001, this act created the Transportation Security Administration (TSA) in the Department of Transportation. The act gives TSA direct responsibility for aviation and all other transportation security.

As demonstrated by the type and number of sources cited, many cyber CIP activities are related to, and overlap with, other aspects of agencies' national security efforts, including homeland security, information security, national security emergency preparedness telecommunications, and continuity of government operations.

Additional Federal Organizations Have CIP-related Responsibilities

Current cyber CIP efforts do not specifically address all potentially relevant critical infrastructure sectors or federal agencies. As mentioned previously, PDD 63 identifies eight sector infrastructures with 13 lead agencies associated with the eight sectors and five special functions. However, PDD 63 and Executive Order 13231 does not specifically address other possible critical sectors such as food supply, chemical manufacturing, and delivery services and their respective federal agency counterparts.

Although important agencies and sectors may not be officially addressed in PDD 63 or Executive Order 13231, a few organizations have stepped forward to address these gaps. For example, the Department of Agriculture, with responsibilities for food safety, recently established a Homeland Security Council, a departmentwide council with the mission of protecting the food supply and agricultural production. Also, a food ISAC has been recently formed by the Food Marketing Institute in conjunction with NIPC. In addition, officials from the designated private-industry sectors for both electricity and water have identified the need to coordinate with the Department of the Interior. These sectors have an interest in the physical and cyber safeguards for dams under Interior's control, because of the water and electrical power they produce. Officials from both sectors noted that this coordination with Interior was just initiated at the beginning of 2002.

Administration officials acknowledge that PDD 63 and Executive Order 13231 are under review for the possible inclusion of additional sectors. The chair of the President's Critical Infrastructure Protection Board told a Senate subcommittee that the critical infrastructure sectors were being reviewed after the September 11 attacks and the subsequent anthrax attacks on the U.S. Capitol. According to the special advisor, industries such as chemical processing, pharmaceuticals, and colleges and universities need to be reevaluated as critical infrastructures. Additionally, officials at the CIAO noted that the concept of critical infrastructures is being reviewed as part of the development of a national strategy, and that additional government functions are being considered for inclusion.

In addition, the proposal to create a Department of Homeland Security also refers to the need to consider additional sectors. According to the proposal, "the Department would be responsible for comprehensively evaluating the vulnerabilities of America's critical infrastructure, including food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the

chemical and defense industries, postal and shipping entities, and national monuments and icons." This proposal is referring to both cyber and physical aspects of our national infrastructure.

Until all relevant infrastructure sectors and lead agencies are clarified, our existing policies for, and possibly our nation's approach to, cyber CIP remain incomplete. The opportunity for ensuring that all relevant organizations are addressed exists in the development of the new national strategy.

Relationships among Cyber CIP Organizations Are Not Consistently Established

Most organizations were able to identify their relationships and coordination activities. This information is presented in appendix II for each organization that could provide it.

However, in reviewing the reported coordination of organizations with key lead entities identified under PDD 63 and Executive Order 13231, we identified that relationships among all organizations performing similar activities (e.g., policy development, analysis and warning) were not consistently established. For example, under PDD 63, the CIAO was set up to integrate the national CIP plan, coordinate a national education and awareness program, and coordinate legislative affairs. Nevertheless, of the organizations conducting policy development activities, only about one-half reported that they coordinated with the CIAO. Of the organizations with research and development functions, none mentioned the OSTP, which was designated the lead coordinator for research and development in both PDD 63 and Executive Order 13231.

Our prior work on the FBI's NIPC, the lead for analysis and warning, is consistent with these examples. Specifically, in April 2001, we reported that NIPC's role had not been clearly articulated and was not being consistently interpreted.[15] PDD 63 describes general goals and provides an outline of the responsibilities assigned to the NIPC. However, discussions with officials in the defense, intelligence, and civilian agencies involved in CIP, and with OMB and the National Security Council, showed that their views of NIPC's roles and responsibilities differed from one another and, in some cases, from those outlined in PDD 63. Several expressed an opinion that this lack

[15]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

of consensus had hindered NIPC's progress and diminished support from other federal agencies.

In recognition of the inconsistent coordination among organizations involved in cyber CIP, President Bush issued Executive Order 13231, "Critical Infrastructure Protection in the Information Age," which acknowledged the need for additional coordination by creating the President's Critical Infrastructure Protection Board to coordinate federal efforts and programs related to the protection of critical infrastructures. Among the board's activities stated in the order are (1) outreach to the private sector and state and local governments; (2) information sharing; (3) incident coordination and crisis response; (4) recruitment, retention, and training of executive branch security professionals; (5) research and development; (6) law enforcement coordination with national security components; (7) international information infrastructure protection; (8) legislation; and (9) coordination with the Office of Homeland Security. The order established 10 standing committees to support the board's work, including committees on incident response coordination and research and development. According to the Office of Homeland Security, the mission of these committees, within the larger mission of the board, is to coordinate programs across government in order to minimize duplication of efforts, create synergies, and maximize resources.

More recently, the Assistant to the President for Homeland Security, in an April 10, 2002, letter to the chairman of the Senate Governmental Affairs Committee, to address a March request from the committee seeking information on homeland security efforts, discussed the need for increased coordination among several key national cyber CIP organizations. The assistant stated that plans for developing a cybersecurity information coordination center are under consideration and that it would be possible for the President's Critical Infrastructure Protection Board, the outreach and awareness component of the NIPC, and the CIAO to be collocated there to better coordinate each organization's duties and responsibilities related to outreach to private industry.

National Strategy to Ensure Coordination Is Being Developed

A missing requirement for implementing the President's Critical Infrastructure Protection Board and improving coordination continues to be the lack of a national strategy that defines organizational roles and relationships. We have been recommending such a strategy for several years, having first identified the need for a detailed plan in 1998. At that time, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles and new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.[16] At that time, we recommended that OMB ensure such coordination.

As mentioned previously, in January 2000, the White House issued its "National Plan for Information Systems Protection" as a first major element of a more comprehensive strategy to be developed. At that time, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal organizations were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.[17]

In September 2001, we continued to report that an underlying deficiency in the implementation of PDD 63 has been the lack of an adequate national strategy that delineates interim objectives and the specific roles and responsibilities of federal and nonfederal organizations involved in CIP.[18] At that time, among other recommendations, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats defines specific roles and responsibilities of organizations involved in CIP and related information security activities. In commenting on a draft of the report, Commerce noted that the administration is reviewing the organizational structures for CIP to ensure coordination of federal government efforts and that it is developing a new national plan.

[16]GAO/AIMD-98-92, Washington, D.C.: Sept. 23, 1998.

[17]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination*, GAO/AIMD-00-268T (Washington, D.C.: July 26, 2000).

[18]GAO-01-822, Washington, D.C.: Sept. 20, 2001.

The national strategy for cyber CIP is still being developed and is now planned to be issued in September 2002. A key contributor to the national strategy will be input from the Partnership for Critical Infrastructure Security, an organization that grew out of PDD 63, consisting of over 60 private-sector companies and associations and 13 federal government agencies. Also contributing to the national plan will be responses to 53 questions categorized into five critical areas of home user and small business, major enterprises, sectors of the national information infrastructure, national-level institutions and policies, and global issues. The questions deal with key computer information issues, including awareness, best practices and standards, accountability, funding, personnel, information sharing, warning, analysis, and incident response and recovery. The President's Critical Infrastructure Protection Board recently distributed the questions over the Internet.

A clearly defined strategy is essential for defining the relationships among the various cyber CIP organizations, integrating cyber CIP activities with existing laws, and ensuring that our national approach to cyber CIP is both coordinated and comprehensive. Without such a detailed strategy, our nation risks not having the appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.

CIP Funds Are Not Separately Appropriated for Most Organizations, and Precise Levels of Spending Cannot Be Ascertained

Most of the organizations in our review do not receive appropriations specifically designated for cyber CIP and, therefore, do not have a process to track these funds. A complicating factor in tracking funds spent on cyber CIP activities is that organizational totals often include funds spent on physical, cyber, and agency-specific CIP activities. Although most organizations cannot readily identify their cyber CIP funding, a few key organizations can since most, or in some cases all, of their operations are related to cyber CIP activities. These organizations include the CIAO, NIPC, the National Institute of Standards and Technology (NIST), and GSA's Federal Computer Incident Response Center (FedCIRC), as highlighted in the February 2002 Office of Homeland Security overview.[19] Table 3 shows the CIP funding identified in the homeland security budget for these four national cyber CIP organizations.

[19]*Securing the Homeland, Strengthening the Nation*, February 2002.

Table 3: Office of Homeland Security Fiscal Year 2002 and 2003 CIP Funding

Dollars in millions

National CIP entity	Fiscal year 2002 base	Emergency supplemental[a]	Fiscal year 2003 proposed
FedCIRC (GSA)	10	0	11
NIPC (FBI)	72	61	125
Computer Security Division (NIST)	11	0	15
CIAO (Commerce)	5	1	7

[a]P.L. 107-38, the Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States: FY 2001.

Source: Office of Homeland Security, *Securing the Homeland, Strengthening the Nation*, February 2002.

Although most organizations are not appropriated CIP funds, OMB has estimated CIP funding levels by department and independent agencies in its *Annual Report to Congress on Combating Terrorism*.[20] According to OMB's report, CIP funds have increased from approximately $1.2 billion in fiscal year 1998 (actual) to approximately $3.9 billion in the President's fiscal year 2003 budget request.

Since September 11, additional funds have been provided or requested for CIP activities related to homeland security, which has further complicated identifying what aspects of CIP activities are funded. In a recent report to the Congress, the Congressional Research Service stated that the fiscal year 2002 estimates are not readily visible in agency budgets or congressional appropriations.[21] The Congressional Research Service added that a detailed breakdown of CIP funds is not available. Without a precise tracking of cyber CIP funding and spending, it is difficult to determine if the federal government is spending its limited cyber CIP resources on the appropriate priorities. However, OMB officials told us that they plan to provide more detailed breakdowns in the future. Such information is also

[20]OMB collects this information for the *Annual Report on Combating Terrorism* as required by P.L. 105-85. By OMB's definition, CIP encompasses the potential threat from equipment failure, human error, weather and natural disasters, and criminal as well as terrorist attacks.

[21]Congressional Research Service, *Critical Infrastructures: Background, Policy, and Implementation*, Updated February 4, 2002.

necessary to enable the CIP Board to make recommendations to OMB on cyber CIP funding, as outlined in Executive Order 13231.

Conclusions

Protecting our nation's critical infrastructure is vital to our national security, economic stability, and public health and safety. PDD 63 established a strong foundation that defined a starting point, and Executive Order 13231 expanded that foundation by tasking a special advisor to the President for cyberspace security to take a leadership role in enhancing our future efforts in that area. The President's recent proposal to create a Department of Homeland Security states that "currently, at least twelve different government entities oversee the protection of our critical infrastructure." However, as our analysis shows, at least 50 organizations are involved in national or multiagency cyber CIP efforts, as well as additional infrastructure organizations that have not yet been officially recognized.

Further, although most organizations could identify their relationships with other key cyber CIP entities, relationships among all organizations performing similar activities (e.g., policy development or analysis and warning) were not consistently established. Without a strategy that identifies responsibilities and relationships for all cyber CIP efforts, our nation risks not having the appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructures.

Finally, most of the organizations in our review do not receive appropriations specifically designated for cyber CIP and, therefore, do not have a process to track these funds. OMB plans to provide more detailed information on this area in the future.

Recommendation

We have previously recommended that the Assistant to the President for National Security Affairs ensure that the federal government's CIP strategy defines the specific roles and responsibilities of organizations involved in CIP and related information security activities. To supplement this recommendation, we recommend that when developing the strategy to guide federal CIP efforts, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the Special Advisor to the President for Cyberspace Security ensure that, among other things, the strategy

- includes all relevant sectors and defines the key federal agencies' roles and responsibilities associated with each of these sectors, and
- defines the relationships among the key CIP organizations.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Special Advisor to the President for Cyberspace Security; the Chief of Staff and General Counsel, Office of Science and Technology Policy (OSTP); the Chief Operating Officer and General Counsel, Federal Emergency Management Agency (FEMA); the Assistant Secretary and Chief Financial Officer, Department of State; and the Director, Audit Liaison Office, Justice Management Division, Department of Justice. The Department of Justice generally concurred with our findings and recommendations (see appendix IV for Justice's written comments); the Special Advisor to the President for Cyberspace Security and the Department of State did not indicate whether they agreed or disagreed; FEMA requested that we add an additional organization, and OSTP disagreed with our statement that none of the R&D organizations coordinated with them. We received oral comments from officials from the Office of Management and Budget; the Environmental Protection Agency; the Departments of Defense, Energy, Health and Human Services, and Treasury; the Federal Communications Commission; the National Science Foundation; and the General Services Administration. Although the written and oral comments varied in scope and detail, they were primarily limited to technical comments on the description of their responsibilities described in appendix II. We have incorporated these changes in the report, as appropriate. These changes included the addition of a few organizations involved in national or multiagency cyber CIP efforts. The Department of Transportation had no comments on a draft of this report, and we did not receive comments from the Department of Commerce.

In written comments on a draft of this report (see app. V), the Special Advisor to the President for Cyberspace Security acknowledged the complexity and importance of coordinating CIP efforts and stated that the President's Critical Infrastructure Protection Board, created under Executive Order 13231 and composed of senior federal officials, coordinates cybersecurity efforts, including aligning roles and responsibilities. The Special Advisor also pointed out that the coordination of federal efforts is only a small part of the overall infrastructure protection challenge since the majority of the U.S. computing power is not owned by the federal government. He added that he is currently coordinating a

national strategy that will address cybersecurity challenges faced by federal, state, and local governments; private companies; infrastructure owners; and home users. We agree that federal coordination is only part of the overall challenge in effectively managing our nation's cyber CIP efforts and look forward to the completion of the national strategy so that all relevant sectors are included and relationships among the government's many players are defined. The Special Advisor also made separate technical comments, which have been incorporated in the report, as appropriate.

In written comments on a draft of this report (see app. VI), OSTP stated that it is inaccurate for us to "imply that consultations are not occurring with the agencies" with R&D responsibilities and that it has exercised its coordination authority for CIP R&D over the past 5 years through regular senior-level interagency meetings. However, when we asked the R&D organizations who they coordinated with, none indicated that they coordinated with OSTP, and OSTP did not specifically identify the R&D organizations in our review. Also, none of these organizations commented on this statement in our draft report that OSTP took exception to. Therefore, we did not make any changes to the report. In addition, OSTP also made separate technical comments that have been incorporated in the report, as appropriate.

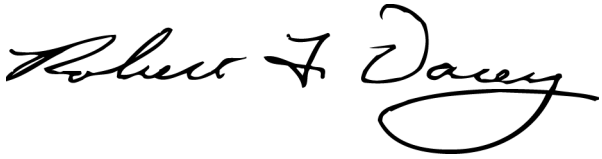
In written comments on a draft of this report (see app. VII), FEMA stated that the current draft does not include the Office of the Chief Information Officer/Information Technology Services Directorate. On the basis of additional information the agency provided in an attachment, we added this office and also incorporated additional technical comments, as appropriate.

In written comments on a draft of this report (see app. VIII), the Department of State did not indicate whether it agreed or disagreed with our draft, but noted that we had not included one of its six organizations, the Bureau of Information Resource Management. We did not include this bureau because it is not involved in national or multiagency cyber CIP efforts. As a result, we made no revisions to our report.

We are sending copies of this report to other interested congressional committees; the Assistant to the President for National Security Affairs; the Assistant to the President for Homeland Security; the Special Advisor to the President for Cyberspace Security; the Director of the Office of

Management and Budget; and the heads of the agencies that are identified in this report. We will also make copies available to others upon request. The report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your offices have any questions about matters discussed in this report, please contact me at (202) 512-3317 or Dave Powner, assistant director, at (303) 572-7316. We can also be reached by e-mail at daceyr@gao.gov or pownerd@gao.gov, respectively. Staff who made key contributors to this report are listed in appendix IX.



Robert F. Dacey
Director, Information Security Issues

Objectives, Scope, and Methodology

The objectives of our review were to (1) identify the federal civilian, defense, and intelligence organizations involved in protecting critical infrastructures from computer-based attacks, and their responsibilities, current organizational placement, and source of authority; (2) determine the organizations' relationships with each other; and (3) determine appropriated critical infrastructure protection (CIP) funds for each organization.

To identify the federal civilian, defense, and intelligence organizations involved in protecting critical infrastructures from computer-based attacks, and their responsibilities, source of authority, and current organizational placement, we selected federal or federally sponsored organizations supporting national or multiagency efforts that were mentioned in either Presidential Decision Directive (PDD) 63 or Executive Order 13231, including lead agencies and members of the President's Critical Infrastructure Protection Board. After identifying the organizations with a national or multiagency cyber CIP effort, we (1) reviewed agency documents including enabling legislation, charters, delegations of authority, policy documents, program and strategic plans, and performance reports; (2) requested written responses from them on their CIP responsibilities, sources of authority, organizational placement and reporting relationships, and funding; (3) interviewed pertinent officials associated with these organizations; and (4) asked for other organizations within these organizations that have a national CIP role. Our inventory of organizations does not include 9 of the 24 largest federal departments or agencies since they were not specifically identified in PDD 63,[22] Executive Order 13231, or by officials we interviewed; organizations that are responsible for the security of critical cyber systems, but do not have national cyber CIP responsibilities outside their agencies, such as the Federal Aviation Administration, the Centers for Disease Control, the Financial Management Service, and the National Weather Service; or agencies that have national physical security CIP responsibilities, such as Treasury's Bureau of Alcohol, Tobacco and Firearms; Transportation's Office of Pipeline Safety; and the Environmental Protection Agency's Chemical Emergency Preparedness and Prevention Office.

[22]These departments or agencies are the Departments of Agriculture, Education, Housing and Urban Development, Interior, Labor, and Veterans Affairs, the U.S. Agency for International Development, the National Aeronautics and Space Administration, and the Nuclear Regulatory Commission.

To determine the organizations' relationships with each other, we (1) reviewed PDD 63 and Executive Order 13231 and written responses regarding organizational placement and reporting relationships; (2) analyzed interdependencies; and (3) held discussions with organization officials and officials from the oversight and policy making bodies such as the Critical Infrastructure Assurance Office (CIAO). We also interviewed the Special Advisor to the President for Cyberspace Security on current initiatives to improve coordination among these organizations.

To determine the level of the organizations' CIP appropriated funds, we analyzed agency budget documents and written responses regarding funding levels. We reviewed recent CIP budget documents created by the Office of Homeland Security, the Office of Management and Budget (OMB), and the Congressional Research Service. We also discussed with OMB how funds are appropriated and tracked for CIP activities.

We performed our work in Washington, D.C., from January through May 2002, in accordance with generally accepted government auditing standards.

Federal Organizations Involved in National or Multiagency Cyber CIP Efforts

The federal organizations listed below have various national or multiagency responsibilities related to cyber CIP efforts. These organizations include 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations. The description of each organization includes its cyber CIP responsibilities, source(s) of authority, key relationships with other CIP organizations, and, where available, information on cyber CIP funds. See figure 4 (in main body of text) for information on organizational placement.

Federal Advisory Committees

Federal Advisory Committees are committees, boards, commissions, or similar groups from the private sector that are established by statute or established or used by the President or one or more agencies for providing advice or recommendations to the President or one or more agencies or federal government officials. Within a year after a presidential advisory committee submits a public report to the President, the President or a delegate of the President is required to report to the Congress proposals for action or reasons for inaction regarding the recommendations contained in the public report. In addition, each year the President is required to provide the Congress with an annual report on the activities, status, and changes in the composition of advisory committees from the preceding fiscal year. According to federal documents, the advisory committees for cyber CIP issues are:

- the National Infrastructure Advisory Council (NIAC),
- the President's Council of Advisors on Science and Technology (PCAST),
- the President's National Security Telecommunications Advisory Committee (NSTAC),
- the President's Information Technology Advisory Committee (PITAC), and
- the National Science and Technology Council (NSTC).

National Infrastructure Advisory Council

Executive Order 13130 established NIAC to advise the President on the security of information systems for critical infrastructure supporting other

sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services. The members of NIAC, which were selected from the private sector, academia, and state and local government, had expertise relevant to the functions of the committee. One of NIAC's main duties was to monitor the development of private-sector information sharing and analysis centers (ISAC). Just before leaving office, President Clinton put forward the names of 21 appointees. The order was rescinded by the Bush Administration before the council could meet. In Executive Order 13231, President Bush established a National Infrastructure Advisory Council (with the same acronym, NIAC) whose functions are similar to those of the council established under the Clinton Administration. The National Infrastructure Advisory Council is comprised of a group of 30 representatives from private industry and state and local government that will advise the President on matters relating to cybersecurity and CIP.

President's Council of Advisors on Science and Technology

A private-sector President's Council of Advisors on Science and Technology assists the National Science and Technology Council to ensure that federal science and technology policies reflect the full spectrum of the nation's needs. Since its creation, the President's Council of Advisors on Science and Technology has been expanded and currently consists of 18 members from the private sector plus the Assistant to the President for Science and Technology, who serves as the committee's co-chair. The committee members, who are appointed by the President, are drawn from industry, education, research institutions, and other nongovernmental organizations.

President's National Security Telecommunications Advisory Committee

Executive Order 13231 calls on the President's National Security Telecommunications Advisory Committee to advise the President on the security and continuity of communications systems essential for national security and emergency preparedness. In 1982, the President's National Security Telecommunications Advisory Committee, which comprises presidentially appointed senior executives from up to 30 major U.S. corporations in the telecommunications and financial services industries, was established to advise the President on national-security and emergency-preparedness telecommunications issues.

President's Information Technology Advisory Committee

Under the authority of Executive Order 13035 (1997) and amended by Executive Order 13092 (1998), the President's Information Technology Advisory Committee provides the President, the Congress, and the federal agencies involved in information technology (IT) research and development with expert, independent advice on advanced information technologies, including the national infrastructure as high-performance computing, large-scale networking, and high-assurance software and systems design. As part of this assessment, the committee reviews the federal networking and IT research and development program. Leading IT experts from industry and academia comprise the committee as it helps guide the administration's efforts to accelerate the development and adoption of information technologies. The committee is formally renewed through presidential executive orders. The current executive order is due to expire June 1, 2003.

National Science and Technology Council

The NSTC was established by executive order in 1993 as a cabinet-level council, with the President serving as chair. This council is the principal means for the President to coordinate science, space, technology, and the various parts of the federal research and development community. An objective of NSTC is establishing clear national goals for federal science and technology. The council prepares research and development strategies that are coordinated across federal agencies to form an investment package aimed at accomplishing multiple national goals. PDD 63 states that the Office of Science and Technology Policy shall be responsible for coordinating research and development programs through the council.

Executive Office of the President

According to federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Office of Homeland Security (OHS),
- the National Security Council (NSC),
- the Office of Science and Technology Policy (OSTP),
- the National Economic Council (NEC),
- the Office of Management and Budget (OMB), and

- the President's Critical Infrastructure Protection Board.

Office of Homeland Security

Established by Executive Order 13228, the mission of the Office of Homeland Security is to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The office, which is led by the Assistant to the President for Homeland Security, coordinates the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. The office identifies priorities and coordinates efforts for collecting and analyzing information. The office also identifies, in coordination with the Assistant to the President for National Security Affairs, intelligence sources outside the United States regarding threats of terrorism within the United States. The office also works with federal, state, and local agencies.

Executive Order 13228 also established the Homeland Security Council which is responsible for advising and assisting the President regarding all aspects of homeland security. The council is to serve as the mechanism for ensuring that homeland-security-related activities of executive departments and agencies are coordinated and homeland security policies are effectively developed and implemented. As previously mentioned, in February 2002, the Office of Homeland Security published an overview of its proposed $37.7 billion fiscal year 2003 budget. This total includes $722 million for technology to defend the homeland, a portion of which is to be allocated to several of the national CIP organizations we identified.

National Security Council

NSC coordinated the initial development and implementation of PDD 63. These efforts included developing the National Information System Defense Plan, monitoring federal agency CIP plans, and fostering a public/private-sector partnership on information assurance. Under the current Bush administration, the council underwent a major streamlining in which all its groups established during previous administrations were abolished. The responsibilities and functions of the former groups were consolidated into 17 policy coordination committees. The activities associated with CIP were assumed by the Counter-Terrorism and National Preparedness Policy Coordination Committee. The Special Advisor to the President for Cyberspace Security reports to the Assistant to the President for National Security Affairs, who leads the council, and to the Assistant to the President for Homeland Security. Furthermore, Executive Order 13231

identifies the Assistant to the President for National Security Affairs as a member of the President's Critical Infrastructure Protection Board.

Office of Science and Technology Policy

The Office of Science and Technology Policy was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976. PDD 63 designates OSTP as the lead agency for research and development for the government through the National Science and Technology Council. Recently, Executive Order 13231 created a standing committee for research and development, which is to be chaired by a designee of the Director of OSTP. This office serves as the primary advisor to the President for policy formulation and budget development on all questions in which science and technology are important elements. The office also leads an interagency effort to develop and implement science and technology policies and budgets that are coordinated across federal agencies. Its Director serves as the Assistant to the President for Science and Technology. In this capacity, the Director manages the National Security and Technology Council and the President's Council of Advisors on Science and Technology.

OSTP's Technology Division is responsible for the following: all of OSTP's activities in the area of emergency-preparedness telecommunications; the NCS; the NSTAC; continuity of government programs; and infrastructure protection programs. In addition, this division works closely with the office's Science Division on national security issues. OSTP's Assistant Director for Homeland and National Security fills the post of Senior Director for Research and Development within the Office of Homeland Security. OSTP's official responsibilities for protecting the domestic infrastructure derive from both statute and executive order. As a result, OSTP coordinates between the military and nonmilitary sectors within the government, between the technical and the policy-making communities, and between the federal government and state and local governments.

National Economic Council

PDD 63 tasked NEC to review sector plans and the national plan for CIP to ensure that they align with the President's economic goals. Additionally, Executive Order 13231 calls on a designee of the chairman of NEC to work in coordination with the chair of the Private Sector and State and Local Government Outreach Committee of the President's Critical Infrastructure Protection Board. NEC was established in 1993 within the Office of Policy Development within the Executive Office of the President to advise the President on matters related to U.S. and global economic policy. By

executive order, NEC has four principal functions: to coordinate policy-making for domestic and international economic issues, to coordinate economic policy advice for the President, to ensure that policy decisions and programs are consistent with the President's economic goals, and to monitor implementation of the President's economic policy agenda.

Office of Management and Budget

Executive Order 13231 calls on a designee of the Director of OMB to chair the Executive Branch Information Systems Security Committee of the President's Critical Infrastructure Protection Board. OMB evaluates, formulates, and coordinates budget and management policies and objectives among federal departments and agencies, including that for information security. Some of its primary responsibilities are to assist the President in developing and maintaining effective government, developing efficient coordinating mechanisms to expand interagency cooperation, and developing regulatory reform proposals and programs. As part of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Congress enacted the Government Information Security Reform Act, tasking OMB with responsibility for establishing and overseeing policies, standards, and guidelines for information security. OMB is also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs.

President's Critical Infrastructure Protection Board

The Special Advisor to the President for Cyberspace Security heads the Office of Cyberspace Security as set forth by Executive Order 13231. The advisor works in close coordination and partnership with the private sector, which owns and operates the vast majority of America's critical infrastructure. The special advisor also reports to the Assistant to the President for Homeland Security and to the Assistant to the President for National Security Affairs. Executive Order 13231 established the President's Critical Infrastructure Protection Board to coordinate the federal efforts and programs associated with protecting our nation's critical infrastructures. The Special Advisor to the President for Cyberspace Security chairs the board. Executive Order 13231 tasks the board with recommending policies and coordinating programs for protecting information systems for CIP. The executive order also established 10 standing committees to support the board's work on a wide range of critical information infrastructure efforts. The board is also intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications that

were assigned to the Office of Homeland Security by Executive Order 13228 of October 8, 2001.

Chief Information Officers Council

The Chief Information Officers (CIO) Council was established by Executive Order 13011 in 1996. As set forth in Executive Order 13231, the vice chair of the CIO Council serves as an official member of the President's Critical Infrastructure Protection Board and sits on the board's coordination committee. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal government agency information resources. The council's role includes developing recommendations for IT management policies, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the federal government's IT workforce. Membership on the council comprises CIOs and deputy CIOs from 28 federal executive agencies. The CIO Council serves as a focal point for coordinating challenges that cross agency boundaries.

National Communications System

Created by Executive Order 12472, the National Communications System's CIP mission is to assure the reliability and availability of national security and emergency preparedness (NS/EP) telecommunications. Its mission includes, but it is not necessarily limited to, responsibility for (1) assuring the government's ability to receive priority services for NS/EP purposes in current and future telecommunications networks by conducting research and development and participating in national and international standards bodies and (2) operationally coordinating with industry for protecting and restoring NS/EP services in an all-hazards environment. NCS's mission is externally focused on the reliability and availability of the public telecommunications network. This mission is carried out within government through the NS/EP Coordinating Committee, with industry on a policy level in coordination with NSTAC, and operationally through the National Coordinating Center for Telecommunications (NCC) and through its participation in national and international standards bodies. Furthermore, in January 2000, NCC was designated an ISAC for telecommunications under the provisions of PDD 63.

NCS reports to the Executive Office of the President–NSC for policy, OSTP for operations, and OMB for budget through the Secretary of Defense, who is the Executive Agent for NCS. NCS's NS/EP Coordinating Committee is a

standing committee under the President's Critical Infrastructure Protection Board. Externally, NCS coordinates with the Office of Cyberspace Security; CIAO; the National Telecommunications and Information Administration; the National Infrastructure Protection Center (NIPC); the General Service Administration's (GSA) Federal Computer Incident Response Center (FedCIRC); the Department of Energy (including several of the laboratories); the Department of Transportation (DOT), industry members of the National Coordinating Center for Telecommunications; ISACs; and numerous Department of Defense (DOD) organizations.

Federal Communications Commission

The Federal Communications Commission (FCC) is an independent U.S. government agency and a nonvoting member of the President's Critical Infrastructure Protection Board. FCC is composed of five commissioners appointed by the President with the advice and consent of the Senate. FCC has the authority to define telecommunications service priorities for national security emergency preparedness when the President has not invoked his wartime authority. In addition, one designated commissioner is assigned responsibility for advising and representing the commission regarding matters of emergency-preparedness and national defense, including national emergency plans and emergency preparedness of private-sector communications organizations and continuity of FCC functions. Recently the commission established an internal advisory body, the FCC's Homeland Security Policy Council, comprising senior managers from each of the FCC's policy, licensing, and operational bureaus and offices. The Homeland Security Policy Council, which serves as an advisory council to the chairman on homeland security matters related to the communications industry, is headed by and reports directly to the chairman's chief of staff. FCC establishes the rules under which the Emergency Alert System (EAS) operates. EAS provides a means of addressing the American people in the event of national emergency. Broadcast stations, cable systems, and participating satellite programmers install equipment that can transmit a presidential message to the public. FCC has created two Federal Advisory Committees to facilitate discussions on infrastructure protection. The Network Reliability and Interoperability Council and the Media Security and Reliability Council advise the commission on incident prevention, system restoration, reliability and public safety issues related to the communications industries.

U.S. Department of Commerce

PDD 63 assigned Commerce as the lead sector liaison for information and communications. Additionally, PDD 63 established a national plan coordination staff, which became the Critical Infrastructure Assurance Office, an interagency office housed in Commerce that is responsible for planning infrastructure protection efforts. Recently, Executive Order 13231 assigned the Secretary of Commerce to the President's Critical Infrastructure Protection Board and established a standing committee for private-sector and state and local government outreach, which is chaired by a designee from Commerce. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Critical Infrastructure Assurance Office (CIAO),
- the National Institute of Standards and Technology (NIST),
- the National Information Assurance Partnership (NIAP), and
- the National Telecommunications and Information Administration (NTIA).

Critical Infrastructure Assurance Office

As established under PDD 63, CIAO performs a variety of CIP functions in three major areas: (1) educating the private sector on the importance of CIP, (2) preparing the national CIP strategy, and (3) assisting federal civilian agencies and departments in determining their dependencies on critical infrastructures.

First, CIAO works to educate industry representatives that critical infrastructure assurance must be addressed through corporate risk management activities. Its efforts focus on the critical infrastructure industries (e.g., information and communications, banking and finance, transportation, energy, and water supply), particularly the corporate boards and chief executive officers who are responsible for setting policy and allocating resources for risk management. In addition to infrastructure owners and operators, this office's awareness and outreach efforts also target members of the audit, insurance, and investment communities. CIAO's goal is to educate these groups on the importance of assuring effective corporate operations, accountability, and information security.

Second, CIAO is tasked with working with government and industry to prepare the national strategy for CIP, which is due for completion in 2002. This strategy will serve as the basis for CIP legislative and public policy reforms, where needed. The development of the national strategy for CIP is to also serve as part of an ongoing process in which government and industry will continuously modify and refine their efforts to ensure the safety of critical information systems.

Third, CIAO is responsible for assisting civilian federal agencies and departments in analyzing their dependencies on critical infrastructures. This mission is conducted under Project Matrix, a program designed to identify and characterize the assets and associated infrastructure dependencies and interdependencies that the government requires to fulfill its most critical responsibilities. Project Matrix involves a three-step process in which each federal civilian agency identifies (1) its critical assets; (2) other federal government assets, systems, and networks on which those critical assets depend to operate; and (3) all associated dependencies on privately owned and operated critical infrastructures.

Additional cyber CIP duties were added to CIAO under Executive Order 13231, including having its director serve as a member of and advisor to the President's Critical Infrastructure Protection Board. CIAO will also support the activities of the National Infrastructure Advisory Council, a group of 30 representatives from private industry and state and local government that will advise the President on matters relating to cybersecurity and CIP. In addition, CIAO will administer a Homeland Security Information Technology and Evaluation Program to study and develop methods to improve information sharing among federal agencies and state and local governments.

CIAO's reported CIP funding to support these activities for fiscal years 2000 through 2002 has been about $4.4 million, $4.8 million, and $6.4 million, respectively.

National Institute of Standards and Technology

NIST is a nonregulatory federal agency within Commerce's Technology Administration that works with industry, federal agencies, testing organizations, standards groups, academia, and private-sector users to improve critical infrastructure security. Policy guidance that directs NIST's CIP-related activities includes Executive Order 13231, the Computer Security Act of 1987, the Government Information Security Reform Act of 2001, and OMB's Circular A-130, Appendix III.

First, NIST supports federal departments and agencies by developing security standards and guidelines for sensitive federal systems as defined under the Computer Security Act of 1987. For example, the institute works with industry to develop voluntary industry standards that support cybersecurity, interoperability, and data exchange. Such standards are to be used to support the operation of the Internet. NIST participants formulate public specifications that assist industry to improve the security and competitiveness of commercial products and to inform consumers.

Second, NIST also helps to improve the security of commercial IT products that provide the communications and information processing backbone of the nation's infrastructure. NIST develops tests, tools, profiles, implementation methods, and recommendations for timely and cost-effective testing programs. Validation programs developed by NIST are conducted in cooperation with private-sector testing laboratories.

NIST coordinates with a wide variety of IT security organizations in the federal government and the private sector. In the federal government, major constituents and collaborators include OMB, the National Security Agency, the General Services Administration, and the departments of Treasury and Health and Human Services. Key interactions include the Federal Public Key Infrastructure Steering Committee and its working groups, the Center for Internet Security, the Federal Computer Security Managers' Forum, the Federal CIO Council, the Committee for National Security, and the Executive Branch Information Systems Security. Examples of IT industry associations with which NIST works include the banking standards community and the Smart Card Consortia. Some key industry collaborations include those with Intel, Microsoft, RSA, IBM, Counterpane Systems, Motorola, Entrust, and Certicom.

NIST's CIP funding to support these activities for 2002 and 2003 has been $11 million and $15 million, respectively.

National Information Assurance Partnership

NIAP is a U.S. government initiative designed to meet the security testing, evaluation, and assessment needs of IT producers and consumers. NIAP collaborates with NIST and the National Security Agency in fulfilling their respective responsibilities under the Computer Security Act of 1987. The partnership, originated in 1997, promotes the development of technical security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. NIAP collaborates with government agencies and industry in a variety of areas to help meet current

and future IT security challenges affecting the nation's critical information infrastructure. One recent NIAP initiative under way is collaborating with industry in developing protection profiles for key information technologies supporting homeland defense.

National Telecommunications and Information Administration

As the lead agency for the information and communications infrastructure sector under PDD 63, Commerce was assigned responsibility for economic security aspects of CIP, which it delegated to NTIA. To fulfill its mission, NTIA conducts five major activities. First, it works to raise the information and communications sector's awareness of cyber vulnerabilities and risks. It then assists this sector in eliminating or mitigating these vulnerabilities. Third, it facilitates the establishment and operation of the information and communications sectors' ISACs. Fourth, it develops partnerships with other countries and international organizations to achieve compatible security policies and strategies. Finally, it provides industry with results from government-based research and development efforts regarding CIP.

To fulfill these responsibilities, NTIA coordinates with a variety of organizations within the government and the private sector. Within Commerce, NTIA coordinates primarily with the CIAO and NIST. Within the federal government, NTIA coordinates with the chair of the President's Critical Infrastructure Protection Board. Within the private sector, NTIA works with three trade associations that serve as sector coordinators: the Information Technology Association of America, the Telecommunications Industry Association, and the United States Telecom Association.

U.S. Department of Defense

PDD 63 identifies national defense as a special function related to CIP and designates DOD as the lead agency for this function. Recently, Executive Order 13231 assigned the Secretary of Defense to the President's Critical Infrastructure Protection Board and established three standing committees that will be chaired or co-chaired by DOD, including the Committee on National Security Systems, the Incident Response Coordination Committee, and the Physical Security Committee. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Joint Staff;

- the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (ASD/C3I);
- the Defense Advanced Research Projects Agency (DARPA);
- the Defense Threat Reduction Agency (DTRA);
- the National Security Agency (NSA);
- the Defense Intelligence Agency (DIA); and
- the Joint Task Force for Computer Network Operations (JTF-CNO).

Joint Staff

The Joint Chiefs of Staff serve as the primary military advisors to the President and, regarding CIP, the chairman of the Joint Chiefs of Staff is responsible for ensuring that critical assets are identified for executing deliberate and crisis action plans and planning for mitigating their loss or disruption. Within the Joint Chiefs of Staff, the Joint Staff serves as special function representative for military plans and operations within the DOD CIP Integration Staff. The Joint Staff is divided into eight directorates: J1-Manpower; J2-Intelligence; J3-Operations; J4-Logistics; J5-Strategic Plans; J6-Command, Control, Communications, and Computers (C4) Systems; J7-Operational Plans; and J8-Force Structure. The J5 CIP office governs the physical aspects of CIP, and the J6 directorate governs the cyber aspects and responsibilities for the Joint Staff.

DOD's Joint Staff coordinates with several organizations, including Combatant Commands; Services; various government agencies; the President's Critical Infrastructure Protection Board, chaired by the Office of Cyberspace Security; the CIAO at Commerce; the NIPC in the FBI; the ASD/C3I; DOT, Office of Security and Intelligence; Office of Homeland Security, Senior Director–Protection and Prevention; the National Security Incident Response Center, chaired by the National Security Agency; the Defense Information Systems Agency; DOD's Computer Emergency Response Teams (CERT); the Joint Task Force Computer Network Defense; FedCIRC; and the Carnegie Mellon CERT® Coordination Center.

The Joint Staff did not receive a specific CIP appropriation before the Defense Emergency Response Funding, which was provided in response to the attacks on September 11. The Joint Staff received $500,000 for CIP

through the Defense Emergency Response Funding that was specifically earmarked for CIP in addition to funds not specifically earmarked for CIP.

Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence

In accordance with PDD 63, DOD is responsible for identifying the national defense infrastructure and working with the national CIP organizational structure and the private sector to ensure its protection. ASD/C3I manages DOD's CIP program and is responsible for its CIP policy development. DOD's CIP program is developing to ensure that critical cyber and physical infrastructure assets that DOD depends on are available to mobilize, deploy, and sustain military operations. ASD/C3I (CIP) develops CIP policy, advocates funding, and oversees implementation of the CIP program. This office oversees DOD's Critical Infrastructure Protection Integration Staff (CIPIS). CIPIS receives input from DOD's defense sectors, lead components, and special function components.

Defense Advanced Research Projects Agency

Executive Order 13231 directs DARPA to work in coordination with the National Science Foundation as members of the President's Critical Infrastructure Protection Board's Committee on Research and Development. In this capacity, DARPA is to assist with federal government research and development for protecting critical infrastructure information systems, including emergency preparedness communications and the physical assets that support such systems, and ensure that government activities are coordinated with corporations, universities, federally funded research centers, and national laboratories. DARPA's Information Technology Office performs research on information technologies for use in advanced defense applications. The office's mission is to provide the networking and computing hardware, software, systems, and management technologies vital to ensuring DOD's military superiority. The office is addressing IT issues of strategic concern, such as security, interoperability, and survivability technologies.

Defense Threat Reduction Agency

Directed by PDD 63, DTRA's CIP-related efforts encompass technology development and combat support. This agency's technology development efforts include managing the development of the National Infrastructure Simulation and Analysis Center (NISAC) and the technical development under its Mission Degradation Analysis (MIDAS) program. NISAC is a joint effort between DTRA and Department of Energy's (DOE) national laboratories to develop an architecture to simulate and analyze the nation's

civilian infrastructures. The MIDAS program is a research effort to determine DOD mission degradation due to degradation in supporting infrastructures. DTRA's combat support efforts include Balanced Survivability Assessments, Joint Staff Integrated Vulnerability Assessments, and the Chemical-Biological Sea Port Protection Analysis.

DITRA's director reports directly to the Assistant to the Secretary of Defense, Nuclear Chemical Biological. Regarding CIP research and development, DTRA coordinates with internal DOD offices and DOE, and has begun to coordinate with the Office of Homeland Security in managing NISAC.

DTRA received appropriations designated for some of its CIP and CIP-related projects for fiscal years 2000, 2001, and 2002, but funding for the remaining CIP efforts were funded through the agency's budgeting process. MIDAS received the following amounts in appropriations: fiscal year 2000, $1.7 million; fiscal year 2001, $2.4 million; and fiscal year 2002, $2.7 million. The Critical Infrastructure Protection Act of 2001, which was enacted as part of the USA PATRIOT Act, authorized $20 million for NISAC for fiscal year 2002. The Balanced Survivability Assessments effort received $8.9 million in fiscal year 2000, $15.8 million in fiscal year 2001, and $17.6 million in fiscal year 2002.

National Security Agency

NSA's primary CIP mission is protecting national security telecommunications and information systems. The Information Assurance Director falls under the purview of the Director, NSA, who is responsible for fulfilling NSA's CIP duties. NSA's IAD performs these duties through assessing the vulnerability of the security of information systems, assessing operations security; evaluating and assessing security measures in national security systems; and addressing the threat, detection, reaction, warning, and response to intrusions into national security systems.

Furthermore, the National Security Incident Response Center is NSA's focal point for addressing computer incidents affecting the U.S. government's national security information systems. The center's CIP duties include providing warnings of threats against U.S. information systems in a timely manner and providing assistance to defense and civil agencies in isolating, containing, and resolving incidents that threaten national security systems. The center also assists the JTF-CNO, FedCIRC, and NIPC in isolating, containing, and resolving attacks and unauthorized intrusions threatening national security systems. NSIRC coordinates its incident reporting and

vulnerability assessments with these entities for attacks and intrusions directed against national security systems. The center's vulnerability assessments are used to develop hardware and software computer network defenses. NSA works with NIST to evaluate commercial off-the-shelf products. In addition, NSA coordinates with the President's Critical Infrastructure Protection Board, the Committee for National Security Systems, and ASD/C3I.

Defense Intelligence Agency

DIA's CIP mission includes collecting and analyzing intelligence data concerning threats to and vulnerabilities of critical infrastructures. A senior staff member of the agency serves as the DOD Intelligence, Surveillance, and Reconnaissance (ISR) CIAO, as well as the Intelligence Special Function Coordinator for all DOD sectors. The ISR CIAO is responsible for developing the ISR Sector Assurance Plan and the ISR Sector Registered Asset List of identified critical assets. These roles are a key element of the DOD-wide CIP program led by ASD/C3I.

DIA received appropriations for some of its CIP and CIP-related projects for fiscal years 2000, 2001, and 2002, but funding for the remaining CIP efforts were funded through the DIA's budgeting process.

Joint Task Force—Computer Network Operations

JTF–CNO, the United States Space Command's operational component for computer network operations, is the primary DOD organization for coordinating and directing internal activities to detect computer-based attacks, contain damage, and restore computer functionality when disruptions occur. JTF–CNO leverages the existing intrusion detection capabilities of the unified commands, its components, and DOD and non-DOD agencies. JTF–CNO receives intrusion data from these sources and integrates these data with intelligence, operational, and technical data. The 2001 JTF–CNO expansion is to allow it to increase JTF–CNO's ability in (1) performing preventative activities, such as conducting security reviews and issuing vulnerability alerts; (2) coordinating and monitoring detection activities performed by components, including monitoring automated intrusion-detection systems; (3) investigating and diagnosing incidents; and (4) handling and responding to events, which involves disseminating information and providing technical assistance to system administrators so that they can appropriately respond to cyberattacks. JTF–CNO maintains a relationship with CERT®/CC, NIPC, and FedCIRC by participating in joint technical exchanges, working groups, and countermeasure development teams.

Director of Central Intelligence

PDD 63 identifies intelligence as a special function related to CIP and designates the Central Intelligence Agency (CIA) as the lead agency for this function. Recently, Executive Order 13231 assigned the Director of Central Intelligence to the President's Critical Infrastructure Protection Board. Additionally, the National Security Act of 1947 designates the Director of Central Intelligence as the primary adviser on national foreign intelligence to the President and the National Security Council, as well as to officials who make and execute U.S. national security policy.

According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Central Intelligence Agency (CIA),
- the National Intelligence Council (NIC), and
- the National Foreign Intelligence Board (NFIB).

Central Intelligence Agency

The CIA's mission is to provide accurate, comprehensive, and timely intelligence on national security topics. PDD 63 directed the CIA to enhance its capabilities to provide intelligence support for threat assessment and warning and to engage in incident response as needed. Since that time, the agency reports that it has made improvements in analytic capabilities and intragovernment coordination regarding mutual analysis, information sharing, and computer incident responses. In addition, the agency established the Information Operations Center to address the growing cyberthreats. CIA involvement in protecting the information infrastructure also extends to participating with other federal agencies and the private sector. In particular, the CIA has assisted the FBI's NIPC by providing technical and analytic support and disseminating cyberthreat assessments. In addition, CIA has collaborated with NIPC and others in the intelligence community to develop and present outreach briefings on foreign cyberthreats to key infrastructure stakeholders, including elements of the private sector.

CIA collects foreign intelligence information through a variety of clandestine and overt means. First, the Directorate of Operations has primary responsibility for the clandestine collection of foreign intelligence. This directorate is divided administratively into area divisions, as well as several staffs, centers, and one division that deals with transnational

issues. Second, the Directorate of Science and Technology (DS&T) provides a wide range of collection support to the CIA and the intelligence community, including human source intelligence collection efforts and agent communications. This directorate supports the National Imagery and Mapping Agency with a cadre of affiliated personnel who serve in key technical positions. Open-source collection (collection of information from foreign radio, television, newspapers, magazines and journals, commercial databases, etc.) is also administered in the DS&T. In addition, this directorate provides collection support for signal intelligence and measurement and signature intelligence.

Once the intelligence has been collected, CIA analysts produce a variety of finished intelligence products that support national-level policy deliberations. The Directorate of Intelligence serves as the executive agency for meeting the bulk of CIA's finished intelligence products for the policy-making community through a number of suboffices, including the Office of Russian and European Analysis; the Office of Near Eastern, South Asian, and African Analysis; the Office of Asian Pacific and Latin American Analysis; and the Office of Transnational Issues. In addition, DS&T produces a number of unclassified products derived from open-source materials.

National Intelligence Council

The National Intelligence Council serves as a senior advisory group to the DCI in his capacity as leader of the intelligence community. This council is responsible for determining and promulgating the intelligence community's judgments on issues of importance to policymakers. Consequently, most of its publications are produced by interagency teams and formally coordinated with all intelligence agencies possessing relevant expertise.

NIC comprises national intelligence officers, experts drawn from all elements of the intelligence community, from outside of government in academia, and from the private sector. National intelligence officers provide mid- and long-term strategic thinking and production by concentrating on substantive problems of particular geographic regions of the world and of particular functional areas (economic and global issues, general-purpose forces, science and technology, strategic programs and nuclear proliferation, and warning). NIC supervises the production of national intelligence estimates and publications, briefs senior policymakers, and focuses intelligence community collection and analytic resources on priority issues. In particular, this council has produced

several documents related to CIP, including a classified 2001 national intelligence estimate on cyberthreats.

National Foreign Intelligence Board

The National Foreign Intelligence Board, an advisory board to the Director of Central Intelligence, has existed in one form or another since the founding of the CIA in 1947. The board includes representatives from all of the agencies that make up the intelligence community (including NIC, CIA, DOD, State, Treasury, FBI, and DOE). In particular, the board is responsible for producing, reviewing, and coordinating national foreign intelligence, and the bulk of its work is to review and approve national intelligence estimates that are created by NIC.

U.S. Department of Energy

PDD 63 assigned DOE as the lead sector liaison for the national energy infrastructure, including electric power and oil and gas production and storage. Recently, Executive Order 13231 assigned the Secretary of Energy to the President's Critical Infrastructure Protection Board and established a standing committee for infrastructure interdependencies, which is co-chaired by designees from DOE and DOT. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Office of Energy Assurance (OEA) and
- the National Laboratories.

Office of Energy Assurance

According to its officials, DOE is currently restructuring the offices that handle security and emergency management for both physical- and cyber-based CIP under the OEA. This office will work with the states and industry to allow for a secure and reliable flow of energy to America's home, industry, and public-service facilities, as well as the transportation system, in direct support of the President's national energy policy and PDD 63.

Three offices will carry out OEA's functions. First, the Office of Energy Reliability coordinates DOE policy development and intergovernmental and interagency activities related to the protection and reliability of the national energy infrastructure. This office will be responsible for developing and maintaining a national strategy for energy assurance in support of the President's national energy policy. It will also provide

leadership for intradepartmental energy-assurance activities and represent DOE in interagency, intergovernmental, and other energy-assurance-related forums. The office will develop a national tracking and reporting process to assess the ongoing effectiveness of the national strategy to identify shortfalls and develop corrective action plans.

Second, the Office of Energy Emergencies will work to ensure that DOE can support state and industry efforts to plan for, respond to, and mitigate actions that disrupt the energy infrastructure. The office will identify potential threats to the national energy infrastructure and communicate information about them to the appropriate authorities to facilitate emergency planning and response. This communications and liaison network will also be maintained during emergencies. The office will develop plans for federal responses to energy emergencies. In addition, the office will assist states and industry by providing technical and professional assistance in the development, testing, and revision of their own emergency response plans.

Third, the Office of Critical Infrastructure Protection will work with national energy organizations within the government and private industry in developing the capability required for protecting the nation's energy infrastructure. The office will assess the vulnerability of the national energy infrastructure to cyber or physical disruptions and identify technologies and capabilities that can protect our nation's critical energy infrastructures and facilitate their use by the private sector and federal agencies. The office will develop and maintain interdependency models and planning tools to assist federal and state government and private industry in anticipating system failures and understanding the cascading effects of single point failures (system failures experienced at centralized network hubs). In addition, the office will coordinate national laboratory research and development programs related to mitigating national energy infrastructure vulnerabilities. This office will be DOE's representative to the Critical Infrastructure Coordination Group and the National Infrastructure Assurance Council.

National Laboratories

DOE funds several national laboratories that conduct CIP-related research. For example, Argonne Laboratories has been working on CIP since 1997 by performing system mapping activities and vulnerability testing. Also, Sandia National Laboratories has established the Information Design Assurance Red Team (IDART). The team works in the areas of information operations and security of critical infrastructures. IDART assessments

evaluate projects and programs for system vulnerabilities in the areas of information warfare, information assurance, and information security.

U.S. Department of Justice

PDD 63 assigned Justice as the lead sector liaison for emergency law enforcement services and for the special function of law enforcement and internal security. Recently, Executive Order 13231 assigned the Attorney General or designee to the President's Critical Infrastructure Protection Board and co-chair of the Incident Response Coordination and Physical Security committees. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Computer Crime and Intellectual Property Section (CCIPS),
- the National Infrastructure Protection Center (NIPC),
- the National Counter Intelligence Executive (NCIX), and
- the Cyber Crime Division.

Computer Crime and Intellectual Property Section

Within the Criminal Division, the CCIPS investigates and prosecutes cyberattacks on our nation's critical infrastructure. This section also addresses policy and legislation issues such as information sharing among the military, the intelligence community, law enforcement, civilian agencies and the private sector, as well as government network intrusion detection and strategic planning. CCIPS coordinates with DOD, CIAO, NIPC, NSC, and interagency groups that work on CIP issues, including work on the national plan to defend cyberspace and the cyber portion of the 5-year counterterrorism plan.

National Infrastructure Protection Center

NIPC, a multiagency organization located within the FBI, detects, analyzes, and warns of cyberthreats to and/or attacks on the infrastructure, should they occur. NIPC's mission is based on authorities given in Executive Order 13231 and PDD 63. In addition, the center is responsible for accomplishing the FBI's role as lead agency for sector liaison for the Emergency Law Enforcement Services Sector. As a sector liaison, NIPC provides law enforcement response for cyberthreats and crimes involving or affecting critical infrastructures. NIPC also facilitates and coordinates the federal

government's response to cyber incidents, mitigating attacks, and investigating threats, as well as monitoring reconstitution efforts. NIPC regularly coordinates with federal, state, local, and law enforcement and intelligence agencies resident in the NIPC: FBI, DOD, CIA, NSA, the United States Secret Service (USSS), Commerce, DOT, DOE, and other federal agencies on the President's Critical Infrastructure Protection Board, as well as Canada and Great Britain.

In addition, NIPC runs the National InfraGard program, which is a cooperative undertaking between the federal government and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of critical infrastructures. InfraGard's goal is to enable the flow of information so that the owners and operators of infrastructure assets, the majority of which are from the private sector, can better protect themselves and so that the U.S. government can better discharge its law enforcement and national security responsibilities. InfraGard provides members a forum for education and training on infrastructure vulnerabilities and protection measures and with threat advisories, alerts, and warnings.

NIPC comprises three sections: (1) the Computer Investigations and Operations Section, which is the operational and response arm and is responsible for designing, developing, implementing, and managing automated tools NIPC uses to collect, analyze, share, and distribute information; and coordinating computer investigations conducted by the FBI's 56 field offices and approximately 400 sublocations throughout the country; (2) the Analysis and Warning Section, which is the indication and warning arm, which provides support during computer intrusion investigations; and (3) the Training, Outreach, and Strategy Section, which provides outreach to the private sector and to local law enforcement, and training and exercise programs for cyber and infrastructure protection investigators within the FBI and other agencies. NIPC's funding to support these activities for fiscal years 2000 through 2002 has been $21 million, $26 million, and $72 million, respectively.

National Counter Intelligence Executive

Executive Order 13231 requires NCIX to coordinate with the President's Critical Infrastructure Protection Board to address threats from hostile foreign intelligence services to programs within the board's purview. Created by PDD 75, "Counterintelligence for the 21st Century," NCIX is appointed by, and reports to, the Director of the FBI, who is the chair of the

Counterintelligence Board of Directors. NCIX serves as the substantive leader of national-level counterintelligence, identifying critical assets, producing strategic counterintelligence analyses, developing a national threat assessment, formulating a national counterintelligence strategy, creating an integrated counterintelligence budget, and developing an agenda of program reviews and evaluations.

Cyber Crime Division

A recent restructuring within the FBI has resulted in a new division called the Cyber Crime Division. The mission of this division has not been finalized.

U.S. Department of Transportation

PDD 63 assigned DOT as the lead sector liaison for aviation, highways, mass transit, pipelines, rail, and waterborne commerce. Recently, Executive Order 13231 assigned the Secretary of Transportation or designee to the President's Critical Infrastructure Protection Board and as co-chair of the Infrastructure Independencies Committee. According to officials, DOT is in the process of establishing the Transportation Security Administration, which was required by the Aviation and Transportation Security Act (P.L. 107-71, Nov. 19, 2001). According to its officials, the department is still determining how CIP responsibilities might be aligned under the new organization. Currently, the Office of Intelligence and Security (OIS) is Transportation's lead office in fulfilling its national CIP responsibilities.

Office of Intelligence and Security

Within the Office of the Secretary of Transportation, OIS analyzes, develops, and coordinates departmental and national policies addressing national defense, border security, and transportation infrastructure assurance and protection issues. The office also coordinates with the public and private sectors, international organizations, academia, and interest groups regarding issues of infrastructure protection, national defense, and drug and migrant interdiction, including serving as the DOT CIP coordinator and sector liaison official under PDD 63 and its lead for both PDD 62 and Executive Order 13231.

Outside DOT, OIS serves the secretary as the transportation sector liaison official under PDD 63. To fulfill this role, OIS establishes sector coordinators, such as the Association of American Railroads and the Airport Councils International–North America, and is the primary liaison

with the Office of Homeland Security, the Office of Cyberspace Security, the intelligence and law enforcement community, and DOD, especially the U.S. Transportation Command. OIS is the transportation sector's primary point of contact for all security issues, including coordinating countermeasures and disseminating threat information.

Environmental Protection Agency

PDD 63 designates the Environmental Protection Agency (EPA) as the lead agency for sector liaison for protecting the water supply. Presidential decision directives 39, 62, and 63 mandate EPA participation in a federal response program specifically aimed at preparing for and responding to terrorist incidents. According to agency officials, EPA and the Office of Homeland Security are currently discussing also designating EPA as the lead agency for sector liaison for chemical preparedness. The Office of Water is the lead EPA office in fulfilling EPA's national CIP responsibilities.

Office of Water

As a result of concerns raised since September 11, the Office of Water has expanded its focus to provide technical and financial assistance for vulnerability assessments, and emergency response planning for drinking water and wastewater utilities. This office also works to improve knowledge and develop new technologies that will help utilities protect assets and public health through cooperative research with other federal agencies and nongovernmental organizations. Finally, the Office of Water facilitates communications among utilities and government officials at all levels regarding preparedness and response activities involving the water sector. In this regard, the office currently is reviewing the interdependencies between areas such as energy, wastewater, and transportation.

Federal Emergency Management Agency

PDD 63 assigned FEMA as the lead sector liaison for the emergency fire service and continuity of government and the responsibility for developing a national infrastructure assurance plan. In addition, Executive Order 13231 assigned the Director of FEMA or designee to the President's Critical Infrastructure Protection Board. FEMA supports state and local emergency-management programs by funding emergency planning, training emergency managers and local officials, conducting large-scale tests, and sponsoring programs that teach the public how to prepare for disasters. According to FEMA officials, the agency's CIP roles are still evolving. In the past, FEMA focused primarily on physical preparedness,

response, and recovery. However, recently, FEMA officials stated that the agency is exploring ways to better help local officials regarding cyber issues. FEMA plans to handle cyberattacks similar to the outreach done for natural disasters. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Office of National Preparedness (ONP),
- the United States Fire Administration (USFA), and
- the Office of the Chief Information Officer (OCIO) and Information Technology Services Directorate.

Office of National Preparedness

Regarding CIP, the Office of National Preparedness provides leadership in coordinating and facilitating all federal efforts to assist state and local emergency-management and emergency-response organizations. The assistance includes planning; training; equipment and exercises necessary to build and sustain the capability to respond to any emergency or disaster, including a terrorist incident involving a weapon of mass destruction, as well as other natural or man-made hazards. This office coordinates with the Office of Homeland Security to develop a national strategy to protect against, respond to, and recover from terrorist threats and incidents that affect the United States and its citizens. To fulfill this goal, the Office of National Preparedness coordinates, integrates, and implements all federal programs and activities that develop, build, and maintain federal, state, and local consequence management capabilities, including first responders. It coordinates, implements, and administers a national capability assurance program that employs standards, assessments, exercises, lessons learned from disasters, and corrective actions to ensure fully interoperable and continually validated federal, state, and local response capabilities. This office also administers grant programs for obtaining the needed levels of consequence management capabilities at the state and local levels of government. ONP's director, who has been designated as the FEMA/CIAO, oversees FEMA's PDD 63 sector responsibilities in support of emergency fire services and continuity of government services.

United States Fire Administration

The United States Fire Administration maintains a CIP information center that serves as the information sharing and analysis center for the emergency fire services sector as envisioned under PDD 63. The center

provides information to over 33,000 local fire and rescue departments, who, as emergency first responders, have the responsibility to prioritize the infrastructures that must be protected from attack. The Fire Administration also maintains the national fire data center, which proposes possible solutions and national priorities, monitors resulting programs, and provides information to the public and fire organizations.

Office of the Chief Information Officer and Information Technology Services Directorate

The Chief Information Officer (CIO) will support FEMA's CIAO in an advisory capacity for all cyber infrastructure protection issues, including those that affect the sectors for which FEMA is the lead agency. As FEMA's executive agency for cybersecurity, the CIO will also support FEMA's CIAO in meeting its PDD 63 responsibilities for internal cyber infrastructure protection. Finally, the CIO will advise the sector liaisons for emergency fire services and continuity of government services on cyber infrastructure issues.

U.S. General Services Administration

Recently, Executive Order 13231 assigned the Administrator of the GSA to the President's Critical Infrastructure Protection Board. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Federal Computer Incident Response Center (FedCIRC) and
- the Office of Acquisition Policy.

Federal Computer Incident Response Center

In support of PDD 63 and the Government Information Security Reform Act, FedCIRC provides a central focal point for computer incident reporting, providing assistance to civilian agencies with independent prevention and response. GSA administers FedCIRC through the Office of Information Assurance and Critical Infrastructure Protection in the Federal Technology Service. FedCIRC's mission is to ensure that the government has critical services available to withstand or quickly recover from attacks against its information resources.

FedCIRC provides the means for federal agencies to work together to handle security incidents, share related information, solve common security problems, collaborate with the President's Critical Infrastructure Protection Board and the NIPC for planning future infrastructure

protection strategies and deal with criminal activities that pose a threat to the critical information infrastructure. FedCIRC distributes advisories and vulnerability notes via e-mail and on its home page, as well as through a quarterly newsletter for information security managers/officers and system administrators.

FedCIRC provides a computer security incident-response service to collect and analyze incident information from all federal civilian agencies. With this service, incidents can be rapidly analyzed so that warnings are issued when a threat is discovered. In addition, FedCIRC researches and analyzes computer incidents and vulnerabilities in detail to identify potential risks to the information infrastructure and works with the IT community to address and resolve these risks. Beginning in June 2002, FedCIRC is offering a "patch authentication and dissemination capability" to identify vendor patches needed to correct known vulnerabilities in agency computer systems. FedCIRC will notify agencies when vulnerabilities are identified, test the patches to verify that they correct the intended vulnerabilities, and make them available to agencies.

FedCIRC's funds specifically appropriated for cyber CIP for fiscal years 2002 and 2003 were $10 million and $11 million, respectively.

Office of Acquisition Policy

PDD 63 tasked GSA, in coordination with Commerce and DOD to assist federal agencies in implementing best practices for information assurance within their individual agencies. In addition, GSA is to identify large procurements related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and, if necessary, propose revisions to the overall procurement process. The Office of Acquisition Policy has a major role in developing, maintaining, issuing, and administering guiding principles via the Federal Acquisition Regulation, which is applicable to all executive branch agencies.

Department of Health and Human Services

PDD 63 appoints the Department of Health and Human Services (HHS) as the lead agency for sector liaison for protection of the health services infrastructure. This role includes public health services and prevention, surveillance, laboratory services, and personal health services. In addition, Executive Order 13231 assigned the Secretary of HHS or designee to the President's Critical Infrastructure Protection Board. Agency officials stated

that the department is experiencing many changes and reorganizations and, as a result, is reexamining its responsibilities for CIP. HHS's Deputy Secretary is charged with overall responsibility for the CIP program, and the department's PDD 63 responsibilities are evolving. The Office of Emergency Preparedness (OEP) is HHS's lead office in fulfilling its national CIP responsibilities.

Office of Emergency Preparedness

The Office of Emergency Preparedness has departmental responsibility for managing and coordinating federal health; medical-and-health-related social services; and recovery to major emergencies and federally declared disasters, including natural disasters, technological disasters, major transportation accidents, and terrorism. As the lead federal agency for health and medical services within the federal response plan, HHS designated this office to work in partnership with FEMA and the federal interagency community. The Office of Emergency Preparedness also directs and manages the National Disaster Medical System, a cooperative asset-sharing partnership between HHS, DOD, the Department of Veteran Affairs, FEMA, state and local governments, private businesses, and civilian volunteers. The office is also responsible for federal health and medical response to terrorist acts involving weapons of mass destruction.

National Science Foundation

The National Science Foundation (NSF) funds CIP-related research in reliable and secure cyber infrastructures, including research on computer and network security and assured information technologies intended to provide sustainable communications and operations in the aftermath of a catastrophic event. NSF's CIP-related funding also includes research on decision science; emergency response and recovery; and the interdependencies and vulnerabilities of physical infrastructure systems, including electrical power, transportation, energy, and water. Under Executive Order 13231, NSF participates in the Critical Infrastructure Protection Board Research and Development Standing Committee and Working Committee and supports studies at the request of the President's Critical Infrastructure Protection Board. Previously, the foundation participated in the interagency Critical Infrastructure Protection Working Group established in response to PDD 63. NSF is involved in other research and development coordination efforts relevant to CIP, including a leadership role in the Information Technology Research and Development Working Group and interaction with the Presidential Information

Technology Advisory Committee. Its responsibilities established under PDD 63 include education for a cybersecurity workforce.

U.S. Department of State

The Department of State advises the President on foreign policy and relations. Accordingly, PDD 63 assigned State as the lead for the special function of foreign affairs, and Executive Order 13231 assigned the Secretary of State or his designee to the President's Critical Infrastructure Protection Board, on which State serves as chair of the International Affairs Committee. According to agency officials and federal documents, the organizations with critical infrastructure protection responsibilities are as follows:

- the Bureau of Resource Management (RM),
- the Bureau of Diplomatic Security (DS),
- the Bureau of Political–Military Affairs (PM),
- the Bureau of International Narcotics and Law Enforcement (INL), and
- the Bureau of Economic and Business Affairs (EB).

Bureau of Resource Management

The Assistant Secretary for Resource Management is responsible for managing the formal department-wide CIP program plan by serving as chair of the Department's Critical Infrastructure Protection Governance Board. The Governance Board facilitates the decision making process on policy and priorities relating to CIP within the Department. In addition, the Resource Management Bureau is responsible for ensuring that the formal departmentwide CIP program is managed and fully resourced over a multiyear planning period to achieve the CIP objectives of PDD 63 for both domestic and overseas operations.

Bureau of Diplomatic Security

The Assistant Secretary for Diplomatic Security is the Department's Chief Infrastructure Assurance Officer, who oversees the protection of all other aspects of the department's critical infrastructure. The Bureau of Diplomatic Security provides a secure environment for conducting American diplomacy and promoting American interest worldwide. Regarding CIP, this bureau develops and maintains effective security

programs for every U.S. embassy and consulate abroad. In addition, the bureau monitors and analyzes intelligence on terrorist activities and threats directed against Americans and U.S. diplomatic facilities overseas, as well as threats against U.S. officials, visiting foreign dignitaries, resident foreign diplomats, and foreign missions in the United States.

Bureau of Political-Military Affairs

The PM Bureau provides policy direction in the areas of international security, military coordination and peace operations, and arms trade. Its responsibilities include developing regional security policy, security assistance, arms transfers, confidence and security building measures, humanitarian de-mining programs, CIP, burden sharing, and complex contingency operations and contingency planning. Regarding federal CIP efforts, this bureau is responsible for coordinating and implementing interagency and intradepartmental policy development. To accomplish this goal, PM leads international cooperation on CIP issues. In addition, Executive Order 13231 assigned this bureau responsibility for the international CIP outreach program. PM's Assistant Secretary serves as State's alternate representative on the President's Critical Infrastructure Protection Board and chair of the Board's International Affairs Committee.

Bureau of International Narcotics and Law Enforcement

INL has specific responsibility for CIP-related issues involving criminal misuse of information technology (e.g., cybercrime). This bureau also coordinates and funds the response of federal law enforcement to requests for training and technical assistance from foreign partners, including assistance in fighting high-technology crime, an important subset of protecting critical networked systems.

Bureau of Economic and Business Affairs

The EB bureau is responsible for CIP-related issues in multilateral economic organizations, such as the Organization for Economic Cooperation and Development, and the Asia Pacific Economic Cooperation forum. In such forums, the bureau works to develop internationally accepted information technology security standards and best practices and to ensure that government information security regimes include input from private stockholders.

U.S. Department of the Treasury

PDD 63 assigned Treasury as the lead sector liaison for banking and finance. Recently, Executive Order 13231 designated the Secretary of the Treasury a member of the President's Critical Infrastructure Protection Board and created the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by the Treasury Assistant Secretary for Financial Institutions. In addition, Executive Order 13228 includes several policy coordinating committees that regularly seek Treasury's input and cooperation. According to agency officials and federal documents, the organizations with national or multiagency cyber critical infrastructure protection responsibilities are as follows:

- the Office of Financial Institutions (OFI),
- the United States Secret Service (USSS),
- the Office of the Comptroller of the Currency (OCC), and
- the Office of Thrift Supervision (OTS).

Office of Financial Institutions

Treasury's Assistant Secretary for the OFI acts as sector liaison to the banking and finance sector on CIP. The office coordinates Treasury's efforts regarding legislation and regulation for financial institutions, federal agencies that regulate or insure financial institutions, and securities markets. In addition, the assistant secretary chairs FBIIC, which coordinates the federal financial regulatory effort to develop a coordinated emergency response mechanism in order to respond to cyber or physical attacks against the financial sector. The OFI also participates on standing committees regarding interdependencies, international outreach, and private-sector outreach. FBIIC has also been tasked by the Office of Homeland Security to examine the possible economic consequences of cyber or physical attacks against these critical assets. Finally, this office is consulting with private-sector representatives to develop a private-sector-driven national strategy for infrastructure assurance, which addresses not only cyberattacks, but also physical attacks against the financial services sector.

United States Secret Service

The United States Secret Service's role in CIP is to lead the research, development, and implementation of effective and innovative investigative programs to combat vulnerabilities of electronic financial transactions and,

as an arm of the Treasury, help sustain a liaison with the banking and finance organizations to assess and address vulnerabilities. To meet this challenge, the Secret Service has permanently assigned representatives to the Critical Infrastructure Assurance Office, NIPC, the Computer Emergency Response Team Coordination Center at Carnegie Mellon, the Office of Homeland Security, and the White House Office of Critical Infrastructure Protection. The Secret Service provides input into the national CIP plan through its representatives in these organizations. The Secret Service has also initiated a nationwide network of Electronic Crimes Task Forces, as mandated by the USA PATRIOT Act. These task forces, which will bring law enforcement, academia, and the private sector together, have been designated to provide a systemic and proactive approach to preventing cyber-based crimes. Regarding physical CIP, the Secret Service helps secure national special security events (e.g., the Olympics).

Office of the Comptroller of the Currency

OCC helps protect the nation's cyber critical infrastructure by chartering, regulating, and supervising national banks to ensure that the banking systems are safe and competitive. To accomplish its goals, OCC approves and denies applications for new national bank charters; examines national banks and other entities subject to its supervision; takes supervisory action against banks that do not comply with laws and regulations; and issues rules, regulations, and supervisory guidance governing a wide spectrum of bank activities, including those relating to investments and lending. The office also participates in the efforts of the FBIIC.

Office of Thrift Supervision

OTS, a Treasury bureau, is the primary regulator of all federal and many state-chartered thrift institutions, which include savings banks and savings and loan associations. Representatives of the OTS are members of the FBIIC.

Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP

Table 4: Executive Department or Agency Components and Their Primary Activities Related to Cyber CIP

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
Federal Advisory Committees					
National Infrastructure Advisory Council	✔				
President's Council of Advisors on Science and Technology	✔				
President's National Security Telecommunications Advisory Committee	✔				
President's Information Technology Advisory Committee	✔				
National Science and Technology Council	✔				
Executive Office of the President					
Office of Homeland Security	✔				
National Security Council	✔				
Office of Science and Technology Policy	✔			✔	
National Economic Council	✔				
Office of Management and Budget	✔				
President's Critical Infrastructure Protection Board	✔				
Chief Information Officers Council	✔				
National Communications System	✔	✔		✔	
Federal Communications Commission	✔		✔		
U.S. Department of Commerce					
Critical Infrastructure Assurance Office	✔				
National Institute of Standards and Technology	✔				✔
National Information Assurance Partnership					✔
National Telecommunications and Information Administration	✔				
U.S. Department of Defense					
Joint Staff	✔				
Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence	✔				
Defense Advanced Research Projects Agency					✔
Defense Threat Reduction Agency		✔			✔
National Security Agency		✔			
Defense Intelligence Agency		✔			

(Continued From Previous Page)

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
Joint Task Force - Computer Network Operations		✔			
Director of Central Intelligence					
Central Intelligence Agency		✔			
National Intelligence Council		✔			
National Foreign Intelligence Board		✔			
U.S. Department of Energy					
Office of Energy Assurance	✔	✔			
National Laboratories					✔
U.S. Department of Justice					
Computer Crime and Intellectual Property Section	✔		✔		
National Infrastructure Protection Center		✔	✔	✔	✔
National Counter Intelligence Executive	✔	✔			
Cyber Crime Division			✔		
U.S. Department of Transportation					
Office of Intelligence and Security	✔				
Environmental Protection Agency					
Office of Water	✔	✔		✔	
Federal Emergency Management Agency					
Office of National Preparedness	✔				
United States Fire Administration	✔				
Office of the Chief Information Officer and Information Technology Services Directorate	✔				
U.S. General Services Administration					
Federal Computer Incident Response Center		✔			
Office of Acquisition Policy	✔				
Department of Health and Human Services					
Office of Emergency Preparedness				✔	
National Science Foundation					✔
U.S. Department of State					
Bureau of Resource Management	✔				
Bureau of Diplomatic Security		✔	✔		
Bureau of Political-Military Affairs	✔				
Bureau of International Narcotics and Law Enforcement			✔		
Bureau of Economic and Business Affairs	✔				

(Continued From Previous Page)

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
U.S. Department of the Treasury					
Office of Financial Institutions	✔				
United States Secret Service	✔		✔		✔
Office of the Comptroller of the Currency	✔		✔		
Office of Thrift Supervision			✔		

Comments from the Department of Justice

U. S. Department of Justice

Washington, DC 20530

May 31, 2002

Joel C. Willemssen
Managing Director
Information Technology Issues
U.S. General Accounting Office
441 G Street, NW
Washington, D.C.

Dear Mr. Willemssen:

On May 17, 2002, the General Accounting Office (GAO) provided the Department of Justice (DOJ) copies of its draft report "CRITICAL INFRASTRUCTURE PROTECTION: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems." The draft was reviewed by representatives of the Criminal Division and the Federal Bureau of Investigation. The DOJ generally concurs with the report and is providing the enclosed minor comments for your consideration and understand that they will be incorporated as appropriate.

I hope the comments will be beneficial in completing the final document. If you have any questions concerning any of the Department's comments (technical or formal) you may contact me on (202) 514-0469.

Sincerely,

Vickie L. Sloan
Director, Audit Liaison Office
Justice Management Division

Enclosure

Comments from the Special Advisor to the President for Cyberspace Security

THE WHITE HOUSE
WASHINGTON

June 7, 2002

Joel C. Willemssen
Managing Director,
Information Technology Issues
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Willemssen:

Thank you for providing me an opportunity to review and comment on the draft GAO report entitled "*CRITICAL INFRASTRUCTURE PROTECTION: Federal Efforts Require a more Coordinated and Comprehensive Approach for Protecting Information Systems*" (GAO-02-474). Coordinating federal critical infrastructure protection (CIP) efforts is a complex and crucial endeavor. In October 2001, the Administration issued Executive Order 13231 creating the President's Critical Infrastructure Protection Board. Composed of senior federal officials, the Board coordinates cybersecurity efforts including aligning roles and responsibilities of the federal departments and agencies.

Your report correctly observes that the risk of computer based attacks is real and growing. However, the coordination of federal efforts is only a small part of the overall challenge of infrastructure protection. The majority of the computing power in the U.S., which is vulnerable to attack or could be comprised and used to launch attacks against the nation's critical infrastructures, is not owned and operated by the federal government; it is owned and operated by private companies (large and small), universities, state and local governments and home users. This presents a unique strategic challenge.

As Chair of the Board, I am coordinating a national strategy on cyber security. The strategy will address a broad spectrum challenges related to cyber security including those faced by federal, state and local governments, as well as, private companies, infrastructure operators and home users.

Sincerely,

Richard A. Clarke
Special Advisor to the President for Cyberspace Security
Chairman, President's Infrastructure Protection Board

Comments from the Office of Science and Technology Policy

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

June 4, 2002

MEMORANDUM FOR JOEL C. WILLEMSSEN
MANAGING DIRECTOR, INFORMATION TECHNOLOGY ISSUES
GENERAL ACCOUNTING OFFICE

FROM: SHANA DALE
CHIEF OF STAFF AND GENERAL COUNSEL

SUBJECT: OSTP Technical Corrections to GAO-02-474

The following are technical corrections to the General Accounting Office's proposed report entitled, "CRITICAL INFRASTRUCTURE PROTECTION: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems."

1) Section entitled, "Relationships Among Cyber CIP Organizations Are Not Consistently Established," paragraph 2, delete sentence 4, "Of the organizations with research and development functions, none mentioned the Office of Science and Technology Policy, who was designated the lead coordinator for research and development in both PDD 63 and Executive Order 13231."

   Comment: OSTP has exercised its coordination authority for CIP over the past five years with those organizations that have research and development (R&D) functions through regular senior level interagency meetings.

   Beginning in March 1998, the National Science and Technology Council formed a Critical Infrastructure Protection Research and Development Interagency Working Group (CIP R&D IWG) under the joint oversight of the Committee on National Security and the Committee on Technology. This CIP R&D IWG, led by OSTP, was established to develop and to sustain a coherent roadmap on technologies that, if implemented within critical national infrastructure sectors, would reduce vulnerabilities and counter threats that could cause major damage to the security, economic vitality, and social well-being of the United States. As a result of PDD-63, the IWG's charter was expanded to develop a process of ongoing R&D planning and appraisal, as well as to provide appropriate R&D support to the Critical Infrastructure Coordinating Group and the national coordinator.

   On October 16, 2001, Executive Order 13231 established a standing committee for research and development (CR&D), chaired by OSTP, to coordinate a program of Federal Government R&D for protection of information systems for critical

2

infrastructure, including emergency preparedness communications and the physical assets that support such systems, and to ensure coordination of government activities in this field with corporations, universities, federally funded research centers, and national laboratories.

The CR&D created under Executive Order 13231 consists of a committee of principals with senior R&D leadership from across departments and agencies. Supporting the CR&D principals is a working level subcommittee with representatives designated by principals from each of the departments and agencies. The committee of principals meets on a quarterly basis, and the subcommittee meets twice monthly. It is inaccurate to imply that consultations are not occurring with the agencies.

2) Appendix II, Executive Office of the President, Office of Science and Technology Policy, paragraph 2, should be modified as follows:

The ~~National Security and International Affairs~~Technology Division is responsible for all of OSTP's activities in the areas of ~~national security and~~ emergency-preparedness telecommunications; the NCS; NSTAC, continuity of government programs; and infrastructure protection programs; and works closely with the Science ~~technology division~~ Division on national ~~information infrastructure protection issues~~security issues. The OSTP Assistant Director for Homeland and National Security fills the post of Senior Director for Research and Development within the Office of Homeland Security. OSTP has official responsibilities for protecting the domestic infrastructure deriving both from statute and executive order. As a result, OSTP coordinates between the military and nonmilitary sectors within the government, between the technical and the policy-making communities, and between the federal government and state and local governments.

3) Appendix III, Components of Executive Departments or Agencies and their Primary Activities Related to Cyber CIP, Executive Office of the President, Office of Science and Technology Policy, should include a check mark in the "Response and recovery" field. (Executive Order 12472, Section 2.)

4) Figure 3: Overview of National or Multi-agency Federal Cyber CIP Organizations, Office of Science and Technology Policy, should include Response and Recovery coloring in addition to Research and Development. (Executive Order 12472, Section 2.)

Comments from the Federal Emergency Management Agency

Federal Emergency Management Agency
Washington, D.C. 20472

June 13, 2002

Mr. Joel Willemssen
General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Willemssen:

FEMA has reviewed General Accounting Office (GAO) Draft Report entitled, CRITICAL INFRASTRUCTURE PROTECTION: *Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GSA-02-474, dated July 2002.

We believe the report, as written does not incorporate the FEMA Critical Infrastructure Protection (CIP) efforts that were approved by Director Joe Allbaugh and submitted to the White House. The current document dilutes the accurate reporting of the Agency's CIP structure and mission. Please substitute the enclosed text for the FEMA portion of your report, page 64.

The report lists and describes the activities of the Office of National Preparedness; Readiness, Response, and Recovery Directorate; and the U.S. Fire Administration as the components of FEMA with activities related to cyber Critical Infrastructure Protection. FEMA's Office of the CIO/Information Technology Services Directorate should be added to that list. Relevant additions are incorporated in the text of the enclosure. The following changes are also required:

1. Figure 4, page 21, should be amended to incorporate the following under "Federal Emergency Management Agency": Office of the CIO/Information Technology Services Directorate.

2. On page 76, Appendix III, "Components of Executive Departments or Agencies and their Primary Activities Related to Cyber CIP," the table should be modified under "Federal Emergency Management Agency" to include an entry, "Information Technology Services Directorate," with a checkmark under Policy Development.

Thank you for the opportunity to review on this report. Our points of contact are Michael Mosteller, ONP, 202-646-4312, and Steve Schmidt, Office of Cyber Security, 540-542-3343.

Sincerely,

Michael D. Brown
Chief Operating Officer/General Counsel

Attachment

Comments from the Department of State

United States Department of State

Washington, D.C. 20520

JUN 11 2002

Dear Ms. Westin:

We appreciate the opportunity to review your draft report, "CRITICAL INFRASTRUCTURE PROTECTION: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information System," GAO-02-474, GAO Job Code 310141.

The Department's comments are enclosed for incorporation, along with this letter, as an appendix to the GAO final report.

If you have any questions regarding this response, please contact Hunter Ledbetter, Office of Intelligence Resources and Planning, Bureau of Resource Management on (202) 647-7231.

Sincerely,

Christopher B. Burnham
Assistant Secretary and
Chief Financial Officer

Enclosure:

As stated.

cc: GAO/IT - Mr. Willemssen
State/OIG - Mr. Berman
State/RM - Mr. Kaplan

Ms. Susan S. Westin,
Managing Director,
International Affairs and Trade,
U.S. General Accounting Office.

GAO Report Revisions

U.S. Department of State

The Department of State (DOS) advises the President on foreign policy and relations. Accordingly, PDD 63 assigned DOS as the lead for the special function of foreign affairs. Executive Order 13231 assigned the Secretary of State or his designee to the President's CIP Board, on which State serves as Chair of the International Affairs Committee. According to DOS documents and officials, there are currently three bureaus within the DOS charged with institutional CIP protection and three others focused primarily on international outreach and coordination involving CIP. These include:

- the Bureau of Resource Management (RM)
- the Bureau of Diplomatic Security (DS)
- the Bureau of Information Management (IRM)
- the Bureau of Political – Military Affairs (PM)
- the Bureau of International Narcotics and Law Enforcement (INL)
- the Bureau of Economic and Business Affairs (EB)

Bureau of Resource Management (RM)

The Assistant Secretary for Resource Management is responsible for managing the formal Department-wide CIP Program plan by serving as Chair of the Department's Critical Infrastructure Protection Governance Board. The Governance Board facilitates the decision making process on policy and priorities relating to CIP within the Department. In addition, the RM bureau is responsible for ensuring that the formal Department-wide CIP Program is managed and resource-loaded over a multi-year planning period to achieve the CIP objectives of PDD-63 for both domestic and overseas operations.

Bureau of Diplomatic Security (DS)

The Assistant Secretary for Diplomatic Security is the Department's Chief Infrastructure Assurance Officer (CIAO) who oversees the protection of all other aspects of the Department's critical infrastructure. The DS bureau provides a secure environment for conducting American diplomacy and promoting American interest worldwide. Regarding CIP, DS develops and maintains effective security programs for every U.S. embassy and consulate abroad.

Bureau of Information Resource Management (IRM)

IRM ensures availability of Information Technology systems and operations, including IT contingency planning, to support the Department's diplomatic, consular, and management operations; it is also the authority for the Department's computer security programs.

Bureau of Political – Military Affairs (PM)

Executive Order 13231 assigned PM responsibility for the international CIP outreach program. PM's Assistant Secretary serves as State's alternate representative on the President's CIP Board and Chair of the Board's International Affairs Committee. In this context, PM is responsible for coordinating and implementing intradepartmental and interagency policy to promote international cooperation on CIP issues.

Bureau of International Narcotics and Law Enforcement (INL)

The INL bureau has specific responsibility for CIP-related issues involving criminal misuse of information technology (e.g. cyber-crime). INL also coordinates and funds the response of federal law enforcement to requests for training and technical assistance from foreign partners, including assistance in fighting high tech crime, an important subset of protecting critical networked systems.

Bureau for Economic and Business Affairs (EB)

The EB bureau is responsible for CIP-related issues in multilateral economic organizations such as the Organization for Economic Cooperation and Development (OECD), and the Asia Pacific Economic Cooperation forum (APEC). In such fora, the EB bureau works to develop internationally-accepted information technology security standards and best practices, and to ensure that government information security regimes include input from private stockholders.

GAO Contact and Staff Acknowledgments

GAO Contact

Dave Powner (303) 572-7316

Acknowledgments

Contributors to this report include Sandra Edwards, Michael Gilmore, Sophia Harrison, Catherine Schweitzer, Jamelyn Smith, and Eric Winter.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

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

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00