

GAO

Report to the Committee on Energy and
Commerce, House of Representatives

February 2003

CRITICAL INFRASTRUCTURE PROTECTION

Challenges for Selected Agencies and Industry Sectors





Highlights of [GAO-03-233](#), a report to the Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

The explosive growth of computer interconnectivity is transforming the workings of our nation, its government, and its critical infrastructures. But with the enormous benefits of this interconnectivity comes a threat: both physical and cyber assets are potentially vulnerable to computer-based attack. In response, Presidential Decision Directive 63 (PDD 63, May 1998) called for a range of actions to improve the nation's ability to detect and respond to serious infrastructure attacks. For specific agencies under the Committee on Energy and Commerce's jurisdiction and for private-sector organizations for which these agencies have responsibilities, GAO was asked, among other things, to assess their progress and challenges in undertaking critical infrastructure protection (CIP) activities.

What GAO Recommends

GAO recommends that the agencies take steps to complete the identification and analysis of their critical assets, including setting milestones and developing plans to address vulnerabilities. GAO also recommends that selected sectors' lead agencies assess the need for public policy tools to encourage increased private-sector CIP activities. In its comments on a draft of this report, HHS concurred with recommended agency activities. Technical comments by other agencies and private-sector entities were also addressed, as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-03-233

To view the full report, including the scope and methodology, click on the link above. For more information, contact Robert Dacey at (202) 512-3317 or daceyr@gao.gov.

CRITICAL INFRASTRUCTURE PROTECTION

Challenges for Selected Agencies and Industry Sectors

What GAO Found

Federal efforts to protect our nation's critical public and private infrastructures have had mixed progress. GAO examined four specific agencies—the Departments of Health and Human Services (HHS), Energy, and Commerce, and the Environmental Protection Agency (EPA)—and found that the agencies have made progress in implementing several PDD 63 requirements, such as appointing chief information assurance officers and preparing initial CIP plans. However, none of the agencies has fully implemented all requirements, including the fundamental processes of identifying agency assets that are critical to the nation and determining their dependencies on other public and private assets, as well as assessing these assets' vulnerabilities. In addition, although most agencies have tentatively identified their critical assets, these efforts could take years to complete given the current pace and estimated time and resource needs. GAO also examined private-sector groups known as Information Sharing and Analysis Centers (ISACs) for five specific industry sectors—information technology, telecommunications, energy, electricity, and water supply. PDD 63 suggested voluntary ISAC creation to, among other things, serve as mechanisms for information sharing between infrastructure sectors and the government. In response, ISACs have been established and are serving as clearinghouses for their sectors to share information. For other suggested activities, such as establishing baseline statistics on computer security incidents (see table below), progress is mixed.

Both the agencies and the ISACs identified challenges and obstacles to undertaking CIP activities. Agency-identified challenges included coordinating security efforts for critical assets with the General Services Administration, which may often be responsible for protecting agency facilities that house critical assets. The ISACs identified obstacles to information sharing, both between the sectors and the government and within the sectors. In particular, they noted concerns that information reported to the government could be subject to public release under the Freedom of Information Act.

ISACs' Progress in Performing Activities Suggested by PDD 63

| Activity | ISAC | | | | |
|--|--------------------|-------------|----------------------------------|----------------------------------|----------------------------------|
| | Telecommunications | Electricity | Information technology | Energy | Water |
| Establish baseline statistics | In progress | In progress | Yes | In progress | In progress |
| Serve as clearinghouse within and among sectors | Yes | Yes | Yes | Only within own sector | Only within own sector |
| Provide library to private sector and government | In progress | Yes | Available only to private sector | Available only to private sector | Available only to private sector |

Source: ISACs.

Contents

Letter

| | |
|---|----|
| | 1 |
| Objectives, Scope, and Methodology | 2 |
| Results in Brief | 4 |
| Background | 7 |
| Agencies Have Not Yet Completed Implementation of CIP Requirements | 25 |
| ISACs' Progress in Implementing PDD 63-Suggested Activities Is Mixed | 39 |
| Efforts to Improve Cooperation and Interaction with ISACs and Assistance to Agencies Continue | 45 |
| PDD 63 Implementation Presents Challenges and Obstacles | 50 |
| Conclusions | 57 |
| Recommendations for Executive Action | 59 |
| Agency Comments and Our Evaluation | 61 |

Appendixes

| | |
|--|----|
| Appendix I: Comments from the Department of Health and Human Services | 63 |
| Appendix II: GAO Contact and Staff Acknowledgments | 66 |
| GAO Contact | 66 |
| Acknowledgments | 66 |

Tables

| | |
|--|----|
| Table 1: Critical Infrastructure Lead Agencies and Sectors | 17 |
| Table 2: Results of Agencies' Implementation of Selected PDD 63 Requirements | 28 |
| Table 3: Tentative Results of Agencies' Efforts to Identify Their Critical Assets | 31 |
| Table 4: Status of Agency Vulnerability Assessments, as of December 2002 | 36 |
| Table 5: Critical Assets Included in Agencies' Continuity-of-Operations/Continuity-of-Government Plans as of December 2002 | 39 |
| Table 6: Overview of Selected Information Sharing and Analysis Centers | 42 |
| Table 7: Entities that Manage and Operate Selected Information Sharing and Analysis Centers | 43 |

| | |
|---|----|
| Table 8: ISACs' Progress in Performing Activities Suggested by PDD 63 | 45 |
| Table 9: Critical Infrastructure Spending by the Departments of Commerce, Energy, and Health and Human Services and the Environmental Protection Agency (Fiscal Years 2001–2003, Dollars in Millions) | 51 |

Figures

| | |
|---|----|
| Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center from 1995 through 2002 | 8 |
| Figure 2: Organizations with CIP Responsibilities, as Outlined by PDD 63 | 13 |
| Figure 3: Computer Security Weaknesses at 24 Major Federal Agencies | 23 |

Abbreviations

| | |
|-------|--|
| CIAO | Critical Infrastructure Assurance Office |
| CIO | chief information officer |
| CIP | critical infrastructure protection |
| DOD | Department of Defense |
| ECIE | Executive Council on Integrity and Efficiency |
| EPA | Environmental Protection Agency |
| FBI | Federal Bureau of Investigation |
| FOIA | Freedom of Information Act |
| GISRA | Government Information Security Reform Legislation |
| GSA | General Services Administration |
| HHS | Department of Health and Human Services |
| IG | inspector general |
| ISAC | information sharing and analysis center |
| NIPC | National Infrastructure Protection Center |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PCIE | President's Council on Integrity and Efficiency |
| PDD | Presidential Decision Directive |
| SCADA | supervisory control and data acquisition |

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.



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

February 28, 2003

The Honorable W.J. "Billy" Tauzin
Chairman, Committee on Energy and Commerce
House of Representatives

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

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, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups. However, this widespread interconnectivity also poses enormous risks to our computer systems and, more important, to the critical operations and infrastructures they support, such as telecommunications, power distribution, national defense, law enforcement, and critical government services. Further, private-sector entities control over 80 percent of our nation's critical infrastructures. Because potential adversaries—be they nation-states, cyberterrorist groups, criminal organizations, or disgruntled insiders—can develop cyberattack capabilities to attempt to exploit these risks, it is essential that our critical infrastructures be adequately protected.

In response to these concerns, in May 1998 the President issued Presidential Decision Directive 63 (PDD 63), which 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 or physical attacks. Such critical infrastructure protection (CIP) activities are intended to enhance the security of cyber and physical public and private infrastructures that are essential to national security, national economic security, or national public health and safety. PDD 63 encouraged nonfederal participation, including voluntary creation of Information Sharing and Analysis Centers (ISACs) to serve as mechanisms for

gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government. The directive also appointed lead federal agencies to work with specific industry sectors, and it established several federal CIP entities, such as the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce, which was intended to, among other things, develop a national plan for CIP, and the National Infrastructure Protection Center (NIPC), an organization within the Federal Bureau of Investigation (FBI) that was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response.

In addition, on October 16, 2001, President Bush issued Executive Order 13231, “Critical Infrastructure Protection in the Information Age,” which continued many PDD 63 activities by focusing on cyberthreats to critical infrastructures; the order also created the President’s Critical Infrastructure Protection Board to coordinate federal cybersecurity efforts. On October 8, 2001, President Bush issued Executive Order 13228, which created the Office of Homeland Security. In addition, on November 25, 2002, the President signed the Homeland Security Act of 2002 creating the Department of Homeland Security, which, among other things, will consolidate certain CIP functions, including assessing the vulnerabilities of and taking necessary measures to protect the key resources and critical infrastructures of the United States.

Objectives, Scope, and Methodology

In response to your requests, our objectives were to

- assess the pace and progress of efforts by the Departments of Health and Human Services (HHS), Energy, and Commerce and by the Environmental Protection Agency (EPA) to implement CIP requirements to protect their own critical infrastructures and assets from cyber and physical attacks, as prescribed by PDD 63 and Executive Orders 13231 and 13228;
- assess the progress of the private-sector ISACs established for the information technology, telecommunications, energy, electricity, and water-supply sectors in achieving the objectives of PDD 63 and Executive Orders 13231 and 13228;
- assess the level of cooperation and interaction between these ISACs and their federal lead agency counterparts, as well as the level of assistance

provided to the selected agencies by CIAO and NIPC and to the ISACs by NIPC; and

- identify any resource-related issues or other challenges or obstacles that the selected agencies and ISACs indicate have affected their efforts to implement the CIP requirements or objectives.

The agencies and ISACs selected for our review were specifically requested by the House Committee on Energy and Commerce as consistent with its jurisdiction for specific agencies and for the industry sectors for which these agencies have responsibilities. We performed this work at the four agencies—HHS, Energy, Commerce, and EPA—and for the five ISACs associated with key sectors of our economy—telecommunications, information technology, electricity, oil and gas energy, and water supply. We also conducted our work at the national CIAO within the Department of Commerce, the Department of Justice and its NIPC, the General Services Administration, and the National Communications System (an interagency body housed within and funded through the Department of Defense).

To assess the pace and progress of efforts by the agencies to implement requirements to protect their own critical infrastructures and assets, we analyzed CIP plans and other documentation of efforts to implement CIP requirements, including current results of their efforts to identify critical assets using CIAO's Project Matrix methodology, where available. Likewise, we evaluated selected vulnerability assessments to determine the methodology used and whether they addressed specific critical assets. We also met with agencies' chief information officers or their staff, chief infrastructure assurance officers, and others responsible for security of the agencies' cyber and physical assets to determine their roles, responsibilities, and current activities. We did not validate the accuracy of data provided in agencies' Project Matrix reports, including their identification of critical assets and vulnerability assessment data. Vulnerability assessments were often physically maintained at the asset location and not readily available, and agencies were also sometimes reluctant to share vulnerability assessments because of their sensitive or classified nature.

To assess the progress and summarize the different management structures and operating principles of private-sector ISACs established for the information technology, telecommunications, energy, electricity, and water-supply sectors, we collected and evaluated relevant ISAC documents such as operational agreements, charters, guidance, reporting requirements,

summary incident statistics, and vulnerability assessments. We also obtained and analyzed information from ISAC officials regarding management structure, operating principles, activities, challenges, obstacles, and level of cooperation and interaction with federal agencies. We did not independently verify information provided by ISAC representatives.

To determine the level of cooperation and interaction between these ISACs and their federal counterparts, as well as the level of assistance that CIAO, NIPC, or both provided to the selected agencies or ISACs, we analyzed available documentation of efforts by CIAO and NIPC to assist the four agencies, and we obtained the views of agency officials about the extent of CIAO and NIPC assistance efforts. In addition, we discussed with officials from Commerce, Energy, EPA, the National Communications System, and NIPC the level of cooperation and interaction between the ISACs and the applicable agencies. We also discussed with ISAC officials the extent of cooperation and interactions with federal agencies.

To determine the identity of any resource-related issues, challenges, or obstacles that the agencies and ISACs indicate have affected their efforts in implementing the CIP requirements or objectives, we analyzed information on CIP budgets and expenditures that the agencies reported to the Office of Management and Budget (OMB) as part of its national security crosscut data call and that was included in OMB's June 2002 combating terrorism report to the Congress. We also analyzed agency documentation on denials of CIP funding requests and obtained pertinent views of agency officials on the adequacy of resources in meeting their CIP responsibilities. We did not validate the accuracy of agency-reported budget data. We also obtained the views of officials in the four agencies and the ISACs on any other challenges or obstacles that have affected their implementation of CIP requirements or objectives.

We conducted our review from March 2002 to February 2003 in accordance with generally accepted government auditing standards.

Results in Brief

All four agencies we reviewed have taken actions to implement federal policy to protect their critical cyber and physical infrastructure from attack, such as appointing a chief infrastructure assurance officer, developing an initial CIP plan, and continuing to establish security awareness and education programs and computer incident response capabilities. However, over 4 years after PDD 63 was issued, the agencies

have still not completed the fundamental step of identifying their critical infrastructure assets and the operational dependencies of these vital assets on other public and private assets. Once these assets and dependencies are identified, further steps will be necessary, such as conducting or updating vulnerability assessments, managing identified vulnerabilities, and ensuring that these assets are appropriately considered in planning for the continuity of essential agency operations. Three of the four agencies have tentatively identified or are revisiting their critical assets, and all four are working to complete this process. However, CIAO and agency estimates show that just to identify the dependencies for one critical asset could take hundreds of staff hours and as much as 6 to 7 months. Further, according to CIAO officials, even its current efforts to streamline the overall process may not require fewer resources to identify asset dependencies. Neither the administration nor the agencies have established specific deadlines or estimated the total resource requirements to complete the asset and dependency identification process, and completing these tasks at the current pace could take years.

Although their basic operations were similar, the five ISACs we reviewed all had different characteristics and had achieved different levels of progress in undertaking the activities suggested by PDD 63. For example, organizations have performed ISAC-related functions, such as sharing computer security incident information and alerts, for the telecommunications and electricity sectors for many years, whereas ISACs for the information technology, water, and energy sectors were only recently established. Also, some ISAC sponsors performed operations in-house, and others hired private contractors to perform these operations. The ISACs estimated different levels of industry participation, which ranged from 60 to 70 percent for one to 90 percent for another. For specific PDD 63-suggested activities, four of the five reported that they had established baseline statistics on computer security incidents, and although all stated that they served as the clearinghouses for their own sectors, two reported that they did not coordinate with other sectors. In addition, three of the five reported that they make historical incident data available to industry partners that have a “need to know” for CIP, but only one makes these data available to the federal government.

Both NIPC and CIAO have provided assistance or information to assist federal agencies in their efforts, and the lead agencies and NIPC have assisted in establishing and operating ISACs. In commenting on their relationship with NIPC, most of the ISACs reviewed were positive, but they identified opportunities for improvement, such as the need for more

warnings and alerts and for providing those warnings on a timelier basis. NIPC officials reported that they are working to address some of these issues and that they have also signed information-sharing agreements with ISACs that contain industry-specific cyber and physical incident-reporting thresholds. Most of these ISACs also reported that they were satisfied with the support they received from their lead agencies.

The federal agencies and ISACs we reviewed identified a number of challenges and obstacles to implementing national requirements and objectives. From the agencies' perspective, these primarily involved obtaining adequate funding and coordinating critical asset protection efforts. ISAC-identified challenges and obstacles included a reluctance to share incident information because of concerns that the government would release it under the Freedom of Information Act and a concern that information sharing within an industry could raise antitrust issues. The recently enacted Homeland Security Act of 2002 includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to the Department of Homeland Security. However, it is too early to tell whether such restrictions will improve information sharing, and whether additional actions may be needed, such as the use of public policy tools, to encourage increased private-sector CIP efforts and information sharing with the federal government.

This report contains recommendations that the agencies take steps to complete the identification and analysis of their critical assets and their dependencies, including setting milestones, developing plans to address vulnerabilities, and monitoring progress. This report also contains recommendations that selected sectors' lead agencies assess the need for public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between industry sectors and the federal government.

The Department of Health and Human Services provided written comments on a draft of this report (see app. I) and concurred with our recommendations for executive agencies, noting that, in many cases, it is already engaged in the recommended activities. We also received written and oral technical comments from the Department of Commerce's CIAO and its National Telecommunications and Information Administration, EPA, HHS, the FBI, the National Communications System, the North American Electric Reliability Council, the Association of Metropolitan Water Agencies, and the Energy and Information Technology ISACs.

Comments from all these organizations have been incorporated into the report, as appropriate.

Background

As our reliance on our nation's critical infrastructures grows, so do the potential threats and attacks that could disrupt critical operations. PDD 63 outlined requirements for federal agencies and suggested activities for the ISACs to encourage a strong partnership between government and the private sector for CIP—requirements and activities emphasized in more recent executive orders and national strategies. PDD 63 calls for the protection of both cyber and physical assets, and cyber CIP continues to be a key component of federal information security efforts.

Incidents, Threats, and Potential Attack Consequences Are Significant

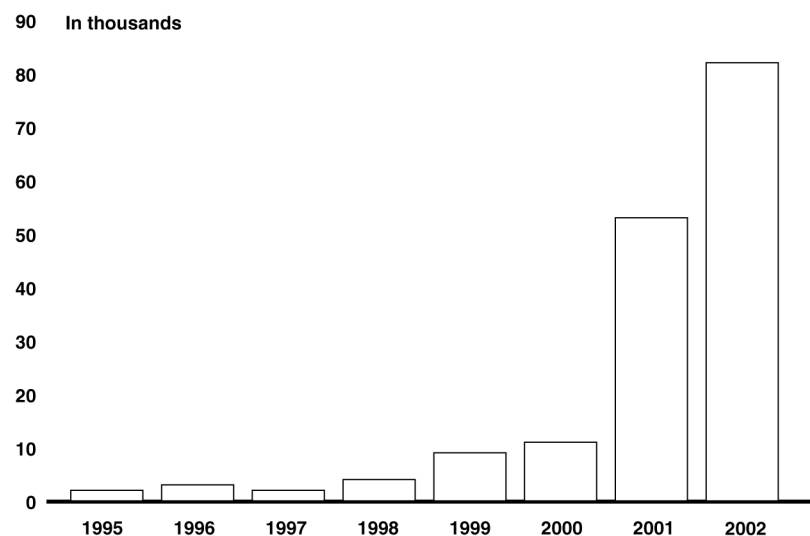
The risks associated with our nation's reliance on interconnected computer systems are substantial and varied. By launching attacks across a span of communications systems and computers, attackers can effectively disguise their identity, location, and intent, thereby making them difficult and time-consuming 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.

The April 2002 report of the Computer Crime and Security Survey, conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches.¹ In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 82,094 in 2002. And these are only the reported attacks. The Director, CERT Centers, stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack, or

¹Computer Security Institute, "2002 Computer Crime and Security Survey," *Computer Security Issues & Trends*, volume VIII, no. 1, Spring 2002.

(2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT Coordination Center from 1995 through 2002.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center from 1995 through 2002



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

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. In February 2002, 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 terrorist groups, such as al Qaeda, has used the Internet to launch a known assault on the infrastructure of the United States, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan.²

²“Administrative Oversight: Are We Ready for A CyberTerror Attack?” Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

Further, in the aftermath of the terrorist attacks of September 11, 2001, there has been an increased recognition of the critical link between cyberspace and physical space. In his November 2002 congressional testimony,³ the Director of the CERT Centers at Carnegie-Mellon University noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions. These computer-controlled and network-connected systems are potential targets for individuals bent on causing massive disruption and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers.

³Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, November 19, 2002.

The September 11, 2001, attacks also raised concerns that potentially disastrous cyberattacks could be coordinated to coincide with physical terrorist attacks to maximize the impact of both. For example, NIPC has warned that the potential for compound cyber and physical attacks, referred to as “swarming attacks,” is an emerging threat to the U.S. critical infrastructure.⁴ As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. A swarming attack could also be used to worsen the effects of a physical attack. For instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. In addition, the recently issued fourth annual report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction concluded that the physical and cyber elements of CIP are so intertwined that it makes no sense to address them separately.⁵

In its October 2002 report, an independent task force cochaired by former Senators Gary Hart and Warren B. Rudman also highlighted the importance of protecting our critical infrastructure from physical attack, noting in particular that our homeland infrastructure for refining and distributing energy to support our daily lives remains largely unprotected against sabotage.⁶ In the report, the task force warned that if the nation does not respond more urgently to address its vulnerabilities, the next attack could result in even greater casualties and widespread disruption to our lives and the economy.

⁴National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (July 2002).

⁵*Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction—IV. Implementing the National Strategy* (Dec. 15, 2002).

⁶*America Still Unprepared—America Still in Danger*, Report of an Independent Task Force Sponsored by the Council on Foreign Relations, released October 2002.

CIP Policy Has Been Evolving Since the Mid-1990s

Federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990s. 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 October 1997, the President's Commission on Critical Infrastructure Protection issued its report,⁷ which described the potentially devastating implications of poor information security for the nation. The report recommended several measures to achieve a higher level of CIP, 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 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 could provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In 1998, the President issued PDD 63, which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. 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 and physical 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 it designated lead agencies to work with private-sector and government organizations. Further, it established CIP 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.

⁷President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (October 1997).

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;⁸

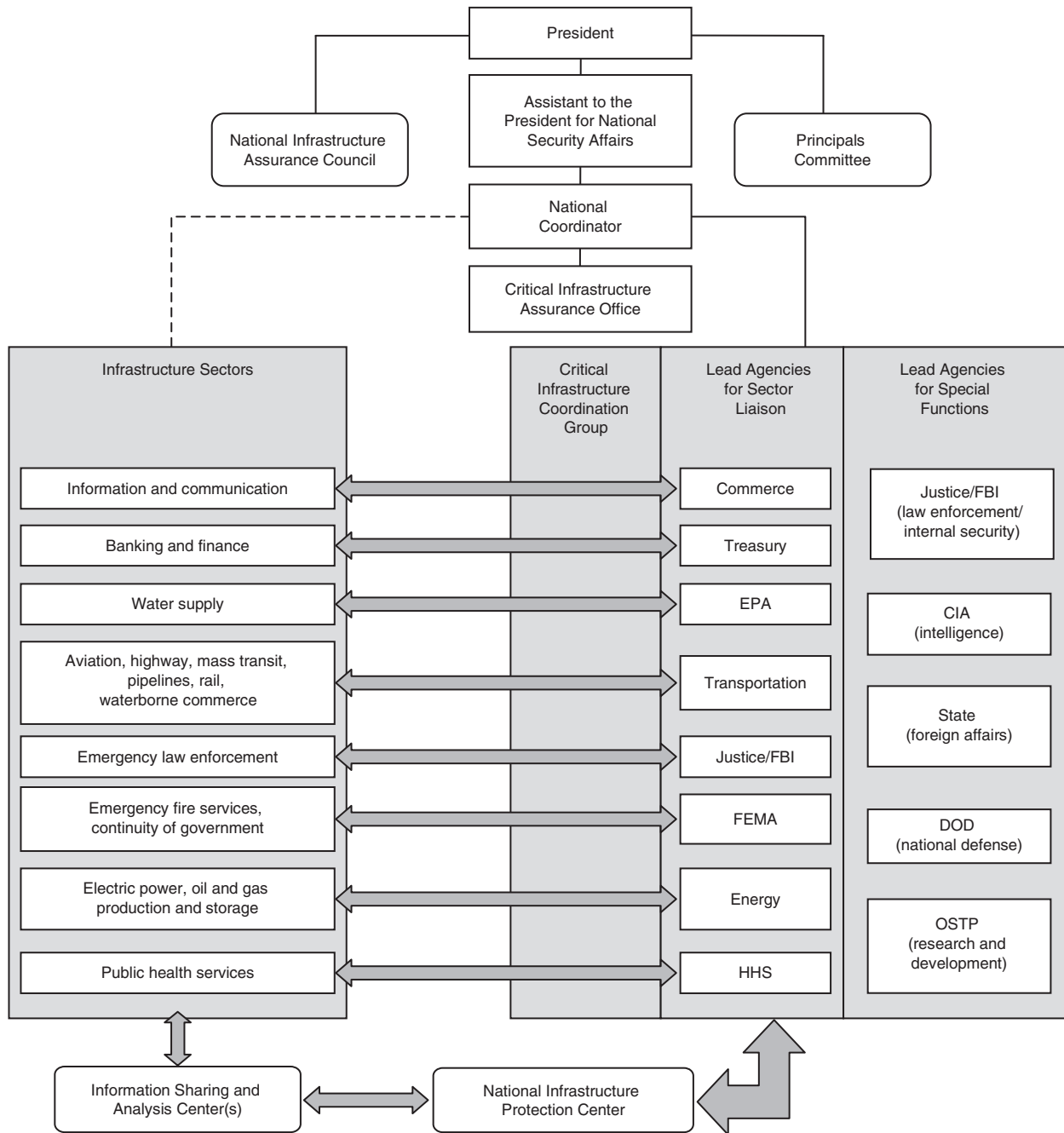
- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and
- the National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.⁹

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. In addition, for each of the infrastructures and functions, the directive designated lead federal agencies (known as sector liaisons) to work with their counterparts in the private sector (known as sector coordinators). To facilitate private-sector participation, PDD 63 also encouraged the voluntary creation of ISACs that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Figure 2 displays a high-level overview of the organizations with CIP responsibilities, as outlined by PDD 63.

⁸PDD 63 created a National Plan Coordination staff responsible for these tasks that, according to CIAO officials, evolved into CIAO.

⁹Executive Order 13231 replaces this council with the National Infrastructure Advisory Council.

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



Source: CIAO.

Note: In February 2001, the Critical Infrastructure Coordination Group was replaced by the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee on Counterterrorism and National Preparedness. In October 2001, the National Infrastructure Assurance Council was replaced by 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.

PDD 63 also called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of infrastructures essential to the operations of the government and the economy. It required that the sector liaison and the sector coordinator work with each other to address problems related to CIP for their sector. In particular, PDD 63 required them to (1) develop and implement a vulnerability awareness and education program and (2) contribute to a sectoral National Infrastructure Assurance Plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and
- developing a plan for alerting, containing, and rebuffering an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

Within the federal government, PDD 63 required every federal department and agency to be responsible for protecting its own critical infrastructure, including both cyber-based and physical assets. To fulfill this responsibility, PDD 63 called for agencies' chief information officers (CIOs) to be responsible for information assurance, and it required every agency to appoint a chief infrastructure assurance officer (who could also be the CIO) to be responsible for the protection of all other aspects of an agency's critical infrastructure. Further, it established the following requirements specifically for or related to federal agencies' protection of their own critical infrastructures:

- develop, implement, and periodically update a plan for protecting its critical infrastructure;
- determine its minimum essential infrastructure that might be a target of infrastructure attack;

-
- conduct and periodically update vulnerability assessments of its minimum essential infrastructure;
 - develop a recommended remedial plan based on a vulnerability assessment that identifies time lines for implementation, responsibilities, and funding; and
 - analyze intergovernmental dependencies, and mitigate those dependencies.

Other PDD 63 requirements for federal agencies are that they provide vulnerability awareness and education to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cybersystems; that they establish a system for responding to a significant infrastructure attack while it is under way, to help isolate and minimize damage; and that they establish a system for rapidly reconstituting minimum required capabilities for varying levels of successful infrastructure attacks.

In January 2000, the White House issued its *National Plan for Information Systems Protection*.¹⁰ 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 physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

In October 2001, 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

¹⁰The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* (Washington, D.C.: January 2000).

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. According to Executive Order 13231, 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. The Special Advisor reports to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security. 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 Director of OMB on issues relating to budgets and the security of federal computer systems. Executive Order 13231 emphasized the importance of CIP and the ISACs, but neither order identified additional requirements for agencies to protect their critical infrastructures or suggested additional activities for the ISACs.

In July 2002, the President issued the *National Strategy for Homeland Security* to “mobilize and organize our nation to secure the United States homeland from terrorist attacks.” According to the strategy, the primary objectives of homeland security, in order of priority, are to (1) prevent terrorist attacks within the United States, (2) reduce America’s vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur.¹¹ In addition, the strategy identifies critical infrastructure and intelligence and warning (critical components of CIP) as two of its six mission areas. It also identifies critical infrastructure sectors that require protection against incapacitation and destruction, including many of the sectors previously identified in PDD 63, such as information and communications, energy, and water, as well as several new sectors, including agriculture, food, chemical and hazardous materials, and postal and shipping.¹² The sectors and their lead agencies are listed in table 1.

¹¹Office of Homeland Security, the White House, *National Strategy for Homeland Security* (July 2002).

¹²NIPC currently reports that 12 ISACs have been formed, including those for the chemicals industry, surface transportation, electric power, telecommunications, information technology, financial services, water supply, oil and gas, emergency fire services, food, emergency law enforcement, and interstate.

Table 1: Critical Infrastructure Lead Agencies and Sectors

| Lead agency | Sectors |
|---------------------------------|---|
| Homeland Security | Information and telecommunications Transportation (aviation; rail; mass transit; waterborne commerce; pipelines; and highways, including trucking and intelligent transportation systems) Postal and shipping Emergency services Continuity of government |
| Treasury | Banking and finance |
| Health and Human Services | Public health (including prevention, surveillance, laboratory services, and personal health services) Food (all except for meat and poultry) |
| Energy | Energy (electrical power, oil and gas production and storage) |
| Environmental Protection Agency | Water Chemical industry and hazardous materials |
| Agriculture | Agriculture Food (meat and poultry) |
| Defense | Defense industrial base |

Source: *National Strategy for Homeland Security* and PDD 63.

The Homeland Security Act of 2002 established the Department of Homeland Security. Regarding CIP, the new department is responsible for, among other things, (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminating, as appropriate, information analyzed by the department both within the department and to other federal agencies, state and local government agencies, and private-sector entities to assist in the deterrence, prevention, preemption of, or response to terrorist attacks. To help accomplish these functions, the act creates the Information Analysis and Infrastructure Protection directorate within the new department and transfers to it the functions, personnel, assets, and liabilities of several existing organizations with CIP responsibilities, including NIPC (other than the Computer Investigations and Operations Section) and CIAO. In addition, as outlined in the *National Strategy for Homeland Security*, the new department will become the lead agency for several industry sectors, including information and telecommunications.

In addition to consolidation of CIP functions and responsibilities within the Department of Homeland Security, the President's fiscal year 2004 budget request for this new department includes \$829 million for information analysis and infrastructure protection, a significant increase from the estimated \$177 million for fiscal year 2003. In particular, funding requested for information analysis and infrastructure protection includes about \$500 million to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that security is improved at these sites. It also includes almost \$300 million for warning advisories, threat assessments, a communications system, and outreach efforts to state and local governments and the private sector.

The *National Strategy for Homeland Security* called for the Office of Homeland Security and the President's Critical Infrastructure Protection Board to complete cyber and physical infrastructure protection plans, which would serve as the baseline for later developing a comprehensive national infrastructure protection plan. This strategy does not indicate a date when the comprehensive plan is to be completed, but on February 14, 2003, the President released the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.¹³

The *National Strategy to Secure Cyberspace* is intended to provide an initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It is also to provide direction to federal departments and agencies that have roles in cyberspace security, and to identify steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. This strategy is organized according to five national priorities, with major actions and initiatives identified for each:

1. **A National Cyberspace Security Response System**—This system is described as a public-private architecture, coordinated by the Department of Homeland Security, for analyzing and warning, managing incidents of national significance, promoting continuity in government systems and private-sector infrastructures, and increasing information-sharing across and between organizations, in order to

¹³The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003); and *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003).

improve cyberspace security. The system is to include governmental entities and nongovernmental entities, such as private-sector ISACs. Major actions and initiatives identified for cyberspace security response include providing for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments; expanding the Cyber Warning and Information Network to support the role of the Department of Homeland Security in coordinating crisis management for cyberspace security; coordinating processes for voluntary participation in the development of national public-private continuity and contingency plans; exercising cybersecurity continuity plans for federal systems; and improving and enhancing public-private information-sharing involving cyber attacks, threats, and vulnerabilities.

2. **A National Cyberspace Security Threat and Vulnerability Reduction Program**—This priority focuses on reducing threats and deterring malicious actors through effective programs to identify and punish them; identifying and remediating those existing vulnerabilities that, if exploited, could create the most damage to critical systems; and developing new systems with less vulnerability, and assessing emerging technologies for vulnerabilities. Other major actions and initiatives include creating a process for national vulnerability assessments, to better understand the potential consequences of threats and vulnerabilities; securing the mechanisms of the Internet by improving protocols and routing; fostering the use of trusted digital control systems/SCADA systems; understanding infrastructure interdependencies and improving the physical security of cybersystems and telecommunications; and prioritizing federal cybersecurity research and development agendas.
3. **A National Cyberspace Security Awareness and Training Program**—This priority emphasizes the promotion of a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace. Other major actions and initiatives include fostering adequate training and education programs to support the nation’s cybersecurity needs; increasing the efficiency of existing federal cybersecurity training programs; and promoting private-sector support for well-coordinated, widely recognized professional cybersecurity certification.

-
4. **Securing Government's Cyberspace**—To help protect, improve, and maintain government's cybersecurity, major actions and initiatives for this priority include continuously assessing threats and vulnerabilities to federal cyber systems; authenticating and maintaining authorized users of federal cyber systems; securing federal wireless local area networks; improving security in government outsourcing and procurement; and encouraging state and local governments to consider establishing information technology security programs and participating in ISACs with similar governments.

 5. **National Security and International Cyberspace Security Cooperation**—This priority identifies major actions and initiatives that can strengthen U.S. national security and international cooperation. These include strengthening cyber-related counterintelligence efforts; improving capabilities for attack attribution and response; improving coordination for responding to cyber attacks within the U.S. national security community; working with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures; and fostering the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from terrorist attacks, and it is based on eight guiding principles. These include establishing responsibility and accountability, encouraging and facilitating partnering among all levels of government and between government and industry, and encouraging market solutions wherever possible and government intervention when needed. The strategy also establishes three strategic objectives. The first is to identify and ensure the protection of the most critical assets, systems, and functions in terms of national-level public health and safety, governance, and economic and national security and public confidence. This would include establishing a uniform methodology for determining national-level criticality. The second strategic objective is to ensure protection of infrastructures and assets facing specific, imminent threats; and the third is to pursue collaborative measures and initiatives to ensure the protection of other potential targets that may become attractive over time. Under this strategy, the Department of Homeland Security will provide overall cross-sector coordination and will serve as the primary liaison and facilitator for cooperation among federal agencies, state and

local governments, and the private sector. In addition, the Office of Homeland Security will continue to act as the President's principal policy adviser staff and coordinating body for major interagency policy issues related to homeland security.

These recently released strategies identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and the Department of Homeland Security, as well as for state and local governments and the private sector. The strategies do not indicate time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives.

Effective Federal Information Security Programs Are Critical to CIP

At the federal level, cyber CIP activities are perhaps the most critical component 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.¹⁴ 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. For the past several years, we have analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.¹⁵ Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.¹⁶

¹⁴U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices.*, [GAO/AIMD-96-110](#) (Washington, D.C.: Sept. 24, 1996).

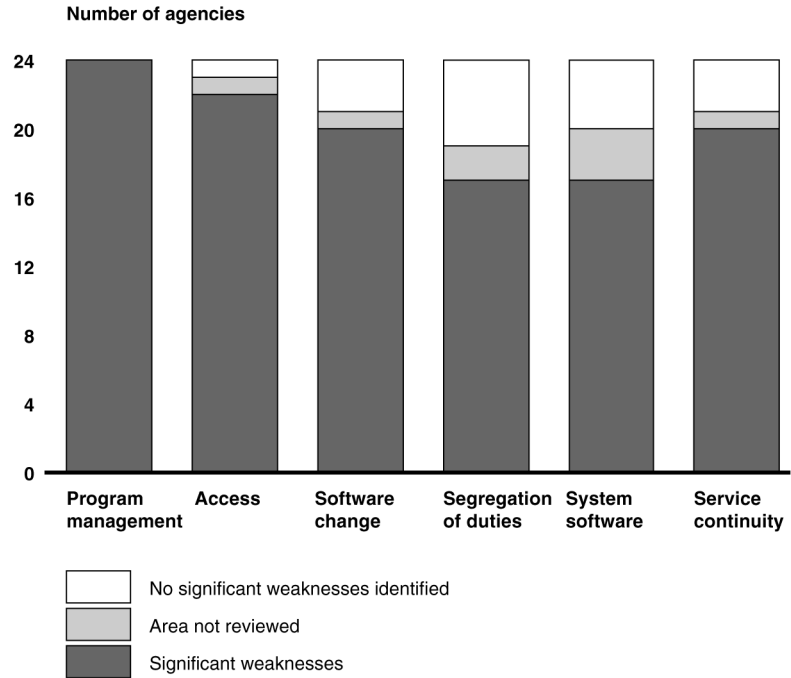
¹⁵U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations Assets at Risk*, [GAO/AIMD-98-92](#) (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, [GAO/AIMD-00-295](#) (Washington, D.C.: Sept. 6, 2000); and *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, [GAO-02-231T](#) (Washington, D.C.: Nov. 9, 2001).

¹⁶[GAO/HR-97-9](#) and [GAO-01-263](#).

Our most recent analyses of audit reports published from October 2001 through October 2002 continue to show significant weaknesses in federal computer systems that put critical operations and assets at risk.¹⁷ Weaknesses continued to be reported in each of the 24 agencies included in our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity’s information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 3 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

¹⁷U.S. General Accounting Office, *Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk*, [GAO-03-303T](#) (Washington, D.C.: Nov. 19, 2002).

Figure 3: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued October 2001 through October 2002.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;

-
- data could be modified or destroyed for purposes of fraud or disruption; and
 - agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Because the weaknesses we identified apply to controls for all or a large segment of an agency's information systems, information security may be no better for agencies' critical infrastructure assets. Further, both we and the inspectors general have reported limited agency progress in implementing PDD 63 requirements to protect critical infrastructures from computer-based attacks. For example, as we reported in September 2001, only limited efforts have been undertaken to perform substantive, comprehensive analyses of infrastructure-sector vulnerabilities and to develop related remedial plans.¹⁸ Also, a March 2001 report by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) identified significant deficiencies in federal agencies' implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by December 2000, and (2) develop procedures and conduct vulnerability assessments.¹⁹ Specifically,

- many agency CIP plans were incomplete, and some agencies had not developed such plans;
- most agencies had not completely identified their mission-essential infrastructure assets; and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

¹⁸U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, [GAO-01-822](#) (Washington, D.C.: Sept. 20, 2001).

¹⁹The PCIE primarily is composed of the presidentially appointed inspectors general, and the ECIE is primarily composed of the agency-head-appointed inspectors general. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 inspectors general of their respective agencies' PDD 63 planning and assessment activities.

In addition, in March 2002 we testified on the efforts by the federal government to implement requirements of the government information security reform legislation (commonly referred to as GISRA),²⁰ and reported that of the 24 large agencies we reviewed, 15 reported that they had not implemented an effective methodology to identify their critical assets.²¹

Agencies Have Not Yet Completed Implementation of CIP Requirements

The four agencies we reviewed (HHS, Energy, Commerce, and EPA) have made progress for several requirements, such as preparing initial CIP plans and appointing chief infrastructure assurance officers. However, none has fully implemented the requirements of PDD 63 to protect its critical cyber and physical infrastructure from attack. In particular, the agencies are still focusing on the fundamental process of identifying their critical assets and these assets' dependencies. Once these assets and dependencies are identified, further steps will be necessary, such as conducting or updating vulnerability assessments, correcting identified vulnerabilities, and ensuring that these assets are appropriately considered in continuity-of-operations planning. Neither the agencies nor the administration has set milestones to complete the asset and dependency identification process or estimated resource requirements, and it could take years to complete these tasks at the current pace.

Initial Progress Has Been Made in Implementing PDD 63 Management Requirements

The four agencies we reviewed have made progress in implementing several PDD 63 requirements to manage their CIP efforts. Specifically, they have all appointed chief infrastructure assurance officers, developed initial CIP plans, and are establishing computer security awareness and education programs and computer incident-response capabilities to respond to cyber attack.

PDD 63 called for CIOs to be responsible for information assurance and required the agencies to appoint chief infrastructure assurance officers to

²⁰Title 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). GISRA has been superseded by the Federal Information Security Management Act, enacted on December 17, 2002, as Title III of the E-Government Act of 2002.

²¹U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, [GAO-02-470T](#) (Washington, D.C.: Mar. 6, 2002).

be responsible for the protection of all other aspects of their critical infrastructure. All four agencies have met this requirement and appointed chief infrastructure assurance officers. The designated chief infrastructure assurance officer is the Director of Headquarters Security Operations within the Office of Security at Energy and the Assistant Secretary for Budget, Technology and Finance at HHS. At Commerce, the CIO is also designated as the chief infrastructure assurance officer, as permitted by PDD 63. At EPA, there are two designated officials or cochief infrastructure assurance officers. According to an official with the Office of Solid Waste and Emergency Response, the assistant administrator for this office was appointed because of the office's responsibility for EPA's national security efforts; and the assistant administrator for the Office of Administration and Resources Management was also appointed because approximately 90 percent of EPA's physical and cyber assets were housed within that office.

PDD 63 also required every department and agency to develop a plan for protecting its own critical infrastructure within 180 days of the issuance of this directive, to implement those plans within 2 years of the issuance of the directive, and to update those plans every 2 years. As required, all four agencies prepared their initial CIP plans. However, although HHS revised its initial plan in October 2000 to incorporate review comments from a CIAO expert review team, none of the agencies has formally updated its plan. HHS and Commerce both intend to update their CIP plans, and in October 2002, HHS awarded a contract that includes this task. However, according to Energy officials and a March 2002 Energy IG report,²² Energy is deferring the updating of its CIP plan until a national-level protection plan is completed. Also, EPA officials indicated that they will defer updating their plan pending further consultation with CIAO.

²²Office of Inspector General, U.S. Department of Energy, *Cyber-Related Critical Infrastructure Identification and Protection Measures*, DOE/IG-0545 (Mar. 20, 2002).

PDD 63 also required the establishment of a system for responding to a significant infrastructure attack while it is under way, with the goal of isolating and minimizing damage. Consistent with PDD 63's cybersecurity emphasis and CIAO guidance highlighting the need to establish a computer security-incident response capability,²³ all four agencies responded that they are establishing incident response capabilities and are reporting incidents to the General Services Administration's (GSA) Federal Computer Incident Response Center.²⁴ Further, HHS's CIO reported that, during fiscal year 2002, the department commissioned an incident response and notification study by a security contractor and will use the results to formulate the next stage of its enterprise security program. Recent IG evaluations required by GISRA confirm most of these agencies' actions to improve incident-handling capabilities. In particular, Commerce's IG reported that a computer incident-response team was established in fiscal year 2002 to provide this capability for operating units that did not have their own, thus ensuring coverage departmentwide. In addition, the EPA IG reported that EPA plans to outsource its incident-handling function.

Another PDD 63 requirement calls for a vulnerability awareness and education program to be established within the government to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cybersystems. Overall, agency efforts related to this requirement primarily focus on information security education and awareness, and all four agencies indicate that they are providing their staff with such training, some of which includes the use of Web-based or automated training tools. However, although IGs' recent GISRA evaluations confirm these efforts, they also reported common weaknesses for these agencies, including that these training programs had not ensured that employees with significant information security responsibilities were receiving adequate training.

Table 2 summarizes the results of the agencies' implementation efforts related to requirements for managing PDD 63 efforts.

²³Critical Infrastructure Assurance Office, *Practices for Securing Critical Information Assets* (January 2000).

²⁴The Federal Computer Incident Response Center provides a central focal point for incident reporting, handling, prevention, and recognition for the federal government. Its purpose is to ensure that the government has critical services available in order to withstand or quickly recover from attacks against its information resources.

Table 2: Results of Agencies' Implementation of Selected PDD 63 Requirements

| Agency | CIP plan | | | Computer incident response capability being established? | Computer security awareness and education program being established? |
|----------|---|------------------|-----------------|--|--|
| | Chief Infrastructure Assurance Officer appointed? | Latest plan date | Update planned? | | |
| HHS | Yes | Oct. 2000 | Yes | Yes | Yes |
| Energy | Yes | Nov. 1998 | No | Yes | Yes |
| EPA | Yes | Apr. 1999 | No | Yes | Yes |
| Commerce | Yes (CIO) | Apr. 1999 | Yes | Yes | Yes |

Source: Department of Health and Human Services, Department of Energy, Environmental Protection Agency, and Department of Commerce (data); GAO (analysis).

Critical Asset Identification Is Still Not Complete

The four agencies we reviewed all provide information and physical security to protect agency assets and reported that they have taken additional protective actions since the terrorist attacks of September 11, 2001, such as increasing guards and building security, performing vulnerability assessments for agency facilities, and updating plans to ensure the continuity of essential operations. However, over 4 years after PDD 63 was issued, the agencies have not completed the fundamental processes of identifying their critical assets and their dependencies on other public- and private-sector assets. Although all four agencies prepared their required initial CIP plans, these plans focused on protecting hundreds of assets considered essential to the agencies' missions rather than focusing on those assets that are critical to the nation.

In October 1998, a month before agencies' initial CIP plans were due, CIAO issued its *Vulnerability Assessment Framework*.²⁵ The framework was intended to provide detailed guidance to federal agencies on how to identify their critical infrastructures, identify interdependencies and vulnerabilities of those infrastructures, and provide the basis for developing remediation plans. However, CIAO officials concluded, on the basis of a review of agency CIP plans and subsequent discussions with agency officials, that agencies did not find the framework particularly helpful in carrying out agency planning efforts. Further, several agencies were unclear whether "critical" organizations, personnel, systems, and facilities to be identified using the framework referred only to those specific missions performed by the individual departments and agencies or more broadly to the performance of functions and missions by federal agencies on behalf of the nation.²⁶

On the basis of this review of the agencies' initial plans, CIAO decided that the management of CIP programs required a new functional approach to defining and identifying critical assets and their dependencies, and it shifted the focus to identifying assets and dependencies that, under PDD 63, are deemed critical to the federal government's carrying out its responsibilities for national security, maintaining the orderly functioning of the national economy, and ensuring the health and safety of Americans. To accomplish this goal and provide the agencies with additional guidance, in March 2000, CIAO began offering its Project Matrix methodology. Project Matrix consisted of a three-step process in which each civilian federal agency identifies (1) its critical assets; (2) other federal government assets, systems, and networks upon which its critical assets depend to operate; and (3) all associated dependencies on private-sector owned and operated critical infrastructures. The Project Matrix methodology defines "critical" as the responsibilities, assets, nodes, and networks that, if incapacitated or destroyed, would jeopardize the nation's survival; have a serious,

²⁵*Vulnerability Assessment Framework 1.1*, prepared by KPMG Peat Marwick LLP for the Critical Infrastructure Assurance Office (October 1998).

²⁶The framework identified two levels of critical organizations, personnel, systems, and facilities, or Minimum Essential Infrastructure (MEI), to be considered and assessed: (1) the national MEI, which provides a flow of goods and services that are absolutely essential to the economic well-being and national security of the United States, to the smooth functioning of governments at all levels, and to society as a whole, and (2) the agency MEI, which provides the inputs and outputs necessary to support the core processes essential to accomplishing an organization's core mission as they relate to national security, national economic security, or continuity of government services.

deleterious effect on the nation at large; adversely affect large portions of the American populace; and require near-term, if not immediate, remediation (currently defined as within 72 hours). It defines “assets” as tangible equipment, applications, and facilities that are owned, operated, or relied upon by the agency, such as information technology systems or networks, buildings, vehicles (aircraft, ships, or land), satellites, or even a team of people.

Once critical assets and their associated dependencies are identified, the agencies are to assess their vulnerability to physical or cyber attack and, if vulnerabilities are found, to develop and implement plans to manage the risks posed by potential attacks to the performance of essential functions and services. Such plans are to seek to deter attacks from happening in the first place, protect critical assets from damage or destruction if attacks occur, mitigate the operational impact of attacks if protective measures fail, restore operations if attacks disrupt services, and reconstitute any assets damaged or destroyed during attacks.

To perform Project Matrix step 1, a CIAO team is to work with the participating agency to identify its PDD 63-relevant assets—that is, pieces of equipment, facilities, or people that are owned, operated, or relied upon by the agency to fulfill its most critical responsibilities. Typically this process includes the team’s conducting document reviews and interviews with selected program managers, to understand how the agency is organized and functions; developing a universal list of physical and cyber assets resident in the agency; producing a revised list of candidate assets by eliminating those not critical to the support of PDD 63 national requirements; and training agency program managers in how to complete an “infrastructure asset evaluation” response for each candidate-list asset. This infrastructure asset evaluation requires the agency to provide answers to a series of questions that describe the asset and its role in supporting the objectives of national or regional security, economic stability, and public health and safety. These responses are then scored by CIAO and, subject to further deliberations by the agency, those with scores that exceed a certain threshold are identified as the agency’s critical assets. Generally, this approach identifies a limited number of critical assets, thus enabling the agency to focus its CIP efforts on those that are most essential to the nation.

All four of the agencies were in some stage of performing Project Matrix step 1 at the time of our review. HHS originally completed step 1 in December 2000 but is now revisiting that analysis given the terrorist

attacks that began on September 11, 2001. For Energy and EPA, CIAO had prepared draft reports for step 1 (dated August 2001 and May 2002, respectively) that presented a compilation of the evaluation responses and resultant analyses and tentatively identified their critical assets. Both agencies are continuing to review and update information in these draft reports. Finally, although Commerce’s 1998–1999 efforts to identify its critical infrastructure assets were the basis upon which Project Matrix step 1 was built, Commerce has now begun to formally perform the step 1 process to refine its list of critical assets.

The agencies we reviewed are all performing the step 1 process and, until they have completed it, their critical assets are only tentatively identified. This is true even for HHS, which recognizes that what is identified as a critical asset may change with different national needs and circumstances, and is revisiting the step 1 process it completed over 2 years ago. Table 3 shows how this process winnows down the total number of agency assets to a handful. The critical assets the agencies tentatively identified include both cyber and physical, and they range from computer centers, laboratories, and buildings to mobile laboratories and teams of experts. However, because of their sensitivity both individually and collectively, we do not specifically identify any of these in this report.

Table 3: Tentative Results of Agencies’ Efforts to Identify Their Critical Assets

| Agency | Universe | Number of candidates | Number of critical assets |
|----------|----------|----------------------|---------------------------|
| HHS | 900 | 97 | 18 |
| Energy | 2,500 | 88 | 14 |
| EPA | 350 | 27 | 18 |
| Commerce | 231 | 42 | 10 ^a |

Source: Department of Health and Human Services, Department of Energy, Environmental Protection Agency, Department of Commerce (data); GAO (analysis).

^aEstimated by Commerce officials based on ongoing Project Matrix step 1 efforts.

In Project Matrix step 2, an agency is to identify the other federal government assets, systems, and networks upon which its critical assets depend to operate. Currently, CIAO plans to assist an agency in analyzing two of its critical assets, and the agency is to perform the analyses for the remaining assets. Two of the four agencies we reviewed had not initiated the next steps of the Project Matrix methodology. Specifically, although

Commerce was a pilot for step 2 in 1999, of the four agencies, only HHS and Energy have begun this step, with CIAO assistance, for a few critical assets. In addition, HHS officials report that the department has awarded a contract to complete step 2 for all of its critical assets.

Further, none of the agencies had begun step 3, in which an agency identifies and analyzes the critical assets' dependencies on nonfederal infrastructures and identifies potential points of failure. Identifying such interdependencies and dependencies is a critical step. For example, Energy officials noted that the Bureau of Reclamation within the Department of the Interior, the Army Corps of Engineers within DOD, and the Tennessee Valley Authority all operate dams that supply electricity to some of Energy's critical assets and that could affect the availability of these assets. This dependency is also an important consideration for these other agencies' CIP efforts, particularly if these agencies have not yet identified such dependencies. For this example, according to CIAO officials, none of these other agencies has undergone a Project Matrix review.

Although the agencies we reviewed are all participating in Project Matrix, it is difficult to estimate when they will complete the process. None of the agencies had estimates of when the individual steps or overall process would be completed or of the total resources that would be required, and CIAO officials emphasized that the actual time to complete a Project Matrix step depends on an agency's priorities and resources.

As an indication of the time required to complete Project Matrix, CIAO officials told us that to assist an agency, CIAO itself requires a total of approximately 1,000 staff hours to complete step 1 and 750 staff hours per asset to complete step 2 (CIAO plans to assist the agencies in analyzing only two of their critical assets for this step). Since no agency has completed step 3, these officials projected that CIAO would also require 250 staff hours per asset for this step. As an indication of the time required to complete Project Matrix from the agency perspective, an HHS official stated that it took 6 to 7 months to complete a step 2 analysis for one of the department's critical assets. Further, Energy officials estimated that it will take 700 hours of staff time and \$100,000 in contract support costs to do step 2 for one critical asset, and they now question whether they will have the funding to complete step 2. On the basis of these estimates, it could take years for these agencies to complete their analyses for all critical assets at their current pace.

In addition to there being no agency Project Matrix completion estimates, there currently is no governmentwide milestone that would indicate when the agencies should complete their analyses other than those in PDD 63 that called for an initial operating capability by the close of 2000 to protect the nation's critical infrastructures from intentional destructive acts, and for an enhanced capability no later than May 2003. In September 2001, we recommended that the federal government's strategy define interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives.²⁷ However, subsequent federal CIP policy and strategy do not contain any specific milestones that would require agencies to complete implementation of requirements. Specifically for Project Matrix, in February 2002 OMB reported to the Congress that it was requiring all large federal agencies to undergo a Project Matrix review²⁸ and, according to a CIAO official, has set a goal of having 31 agencies complete Project Matrix. However, OMB did not establish a deadline for these reviews to be completed. As of July 2002, CIAO reported that of the 31 agencies targeted, 18 had begun their reviews, and of those, only 5 are shown as completing step 1 (including HHS, for its December 2000 results) and only 5 had begun step 2 (includes HHS and Energy).²⁹ CIAO's deputy director said that this office's current goal is to complete Project Matrix reviews for 24 of the 31 identified agencies by the end of fiscal year 2004 and for the remaining 7 in fiscal year 2005. However, this goal is internal to CIAO and has not been communicated to the agencies.

Finally, the CIAO deputy director told us that at the request of the Office of Homeland Security, CIAO is currently revising and streamlining its Project Matrix methodology to approach step 1 from a high-level functional basis that would be less labor intensive for the agencies instead of from the level of the individual asset owners. In addition, the revision would combine the identification of these assets' dependencies on other government and private-sector assets (formerly steps 2 and 3) as step 2. This official estimated that under the new streamlined methodology, step 1 would take an agency from 8 to 12 weeks to complete, depending on its size. He could

²⁷[GAO-01-822](#).

²⁸Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform* (February 2002).

²⁹CIAO also reported that two other agencies found no candidate assets to undergo a step 1 process.

not, however, estimate whether the new combined step 2 would require less time or resources for CIAO or the agencies.

Agencies' Efforts to Implement PDD 63 Requirements for Critical Assets Are Also Incomplete

Several PDD 63 requirements related to the agencies' protection of their own critical infrastructures are dependent on agencies' identification of critical assets, including conducting and periodically updating vulnerability assessments, developing a recommended remedial plan based on vulnerability assessments, and rapidly reconstituting minimum required capabilities for successful infrastructure attacks. Data collected by the agencies for Project Matrix show that agencies' efforts to implement these requirements for all critical assets are incomplete and do not ensure that critical asset vulnerabilities are identified and corrected, and that these assets are appropriately considered in planning for the continuation of critical operations.

PDD 63 requires agencies to conduct vulnerability assessments for their critical assets, and federal vulnerability assessment guidance requires that these vulnerability assessments be periodically updated. The four agencies we reviewed and CIAO identified several sources of guidance for conducting vulnerability assessments for cyber assets, including CIAO's October 1998 *Vulnerability Assessment Framework*, its January 2000 *Practices for Securing Critical Information Assets*, and NIST's October 2001 *Risk Management Guide for Information Technology Systems*.³⁰ As defined in CIAO's January 2000 guidance, a cyber vulnerability assessment is an examination of the ability of a system or application (including current security procedures and controls) to withstand assault, and this examination may be used to (1) identify weaknesses that could be exploited and (2) predict the effectiveness of additional security measures in protecting information resources from attack. With regard to assessing the vulnerability of physical facilities, all four agencies indicated that they used a 1995 study by the U.S. Marshals Service, which provides recommended minimum security standards for five different building security levels.³¹ These levels are based primarily on staffing size, number of employees, use, and the need for public access, but the determination of

³⁰National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, October 2001.

³¹U.S. Marshals Service, Department of Justice, *Vulnerability Assessment of Federal Facilities* (June 28, 1995).

the security level for a facility also considers threat intelligence, crime statistics, and agency mission. Neither PDD 63 nor the above guidance specifies an interval for how often these assessments should be updated, but the guidance does indicate that updates should be performed when significant changes occur. However, guidance by GSA's Federal Protective Service does call for periodic vulnerability surveys for facilities according to their security levels, with frequencies ranging from every 4 years for level 1 and 2 facilities to every 2 years for more sensitive level 4 facilities.

For the three agencies we reviewed that had tentatively identified their critical assets (Energy, EPA, and HHS), data collected by the agencies in performing Project Matrix step 1 showed that their vulnerability assessment efforts are incomplete.³² As indicated by the agencies, the critical assets are characterized as cyber only, physical only, or both cyber and physical. As a result, some assets required either a cyber or physical vulnerability assessment, and others required both. Table 4 summarizes these vulnerability assessment data for these three agencies, through December 2002. First, it shows that none of the agencies had completed cyber or physical vulnerability assessments for all of its assets. For example, of HHS's 15 critical assets with cyber characteristics, 10 (or 67 percent) had cyber vulnerability assessments. Table 4 also shows that for the vulnerability assessments that were performed, HHS and Energy had a number of both cyber and physical vulnerability assessments that were 2 years old or older. These older assessments predate the September 11th attacks, which experts agree represent a significant change in threat and attack scenarios. In addition, for Energy, these older vulnerability assessments were conducted before the assets were tentatively identified as critical.

³²Commerce had not yet identified its critical assets, but for its 42 identified candidate assets, Commerce-provided data indicated that not all had current cyber and physical vulnerability assessments.

Table 4: Status of Agency Vulnerability Assessments, as of December 2002

| Vulnerability assessment status | HHS | | Energy | | EPA | |
|--|-----|-------|--------|-------|-----|-------|
| Critical assets tentatively identified ^{a, b} | 18 | | 14 | | 18 | |
| Number requiring cyber assessment | 15 | (83%) | 12 | (86%) | 3 | (17%) |
| Number requiring physical assessment | 11 | (61) | 13 | (93) | 18 | (100) |
| Cyber vulnerability assessments | | | | | | |
| Completed | 10 | (67) | 7 | (58) | 2 | (67) |
| Number completed 2 years old or older | 2 | (20) | 3 | (43) | 1 | (50) |
| Physical vulnerability assessments | | | | | | |
| Completed assessments | 10 | (91) | 8 | (62) | 13 | (72) |
| Number completed 2 years old or older | 5 | (50) | 3 | (38) | 0 | (0) |

Source: Department of Health and Human Services, Department of Energy, Environmental Protection Agency (data); GAO (analysis).

^aCommerce had not yet tentatively identified its critical assets.

^bAgencies identified critical assets to be cyber only, physical only, or both cyber and physical. Thus, some assets required either a cyber or physical vulnerability assessment, and others required both.

In addition to not conducting or updating vulnerability assessments, our analyses of assessments for selected critical assets showed that some physical assessments were not prepared specifically for those assets. Rather, the physical vulnerability assessments we analyzed at HHS, EPA, and Energy sometimes pertained to overall facilities or buildings, and it was not clear to what extent physical vulnerabilities were assessed for a specific critical asset housed within those facilities or buildings. EPA officials reported that because EPA used the U.S. Marshals Service study as the standard for assessing the facilities or buildings that house most of its critical assets, they believe that the physical infrastructure vulnerabilities associated with these critical assets were properly assessed. We agree that these vulnerability assessments did indicate the facility levels assigned according to criteria in the U.S. Marshals Service study. However, these assessments still did not indicate that critical assets housed in a facility or building were explicitly considered either in determining the facility levels or in assessing the threats, vulnerabilities, or risk levels for these facilities. As a result, based on the reported assessment results, we were unable to determine whether physical infrastructure vulnerabilities associated with critical assets had been properly assessed.

All four agencies, including Commerce, are continuing their vulnerability assessment efforts, but it was difficult to estimate when these efforts would provide current assessments for all assets. For example, both EPA

and Energy identified teams of people as critical assets and indicated that they needed additional guidance to conduct vulnerability assessments for these assets. Further, the agencies generally had no system or organization that routinely monitored the status of both cyber and physical vulnerability assessments for their critical assets. Instead, they usually relied on obtaining these data from the asset owners on an ad hoc basis. This practice sometimes resulted in conflicting data between different agency organizations. For example, officials in the HHS Office of Information Resources Management and its Office of Real Property and Management provided conflicting dates for when some physical vulnerability assessments had been completed, which they reconciled at our request.

All four agencies stated that they prepared remedial plans on the basis of individual vulnerability assessments, as required by PDD 63, and that the organization responsible for the asset was responsible for ensuring that identified vulnerabilities are managed. In addition, for cyber-related vulnerabilities, CIO officials from the four agencies all stated that identified information security weaknesses are reported and monitored as part of their tracking of information security corrective actions for GISRA. Recent GISRA independent evaluations conducted by these agencies' IGs generally confirmed that the agencies do have processes for tracking their information security weaknesses. Further, some agencies are reporting overall progress in correcting identified information security weaknesses. For example, although neither their IGs nor we have validated corrective actions, both Commerce and EPA officials report that they have corrected most information security weaknesses identified in our latest audit reports on their computer operations.³³ However, despite this potential progress for cyber vulnerabilities, agency officials acknowledge that they do not have a comparable process to track corrective actions for vulnerabilities identified through physical vulnerability assessments, nor do they ensure that all cyber and physical vulnerabilities and corrective actions are monitored specifically for their critical assets.

³³U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*, [GAO-01-751](#) (Washington, D.C.: Aug. 13, 2001), and *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk*, [GAO/AIMD-00-215](#) (Washington, D.C.: July 6, 2000).

In addition to assessing and correcting their vulnerabilities, PDD 63 requires the rapid reconstitution of agencies' minimum required capabilities—that is, their critical assets. However, data reported by the agencies showed that only one of the three agencies with tentative critical assets (EPA) had included all these assets in its continuity-of-operations plans—plans that provide for the continued performance of essential federal functions (see table 5 below).³⁴ Part of the data collected by the agencies for Project Matrix step 1 concerns whether an asset is included in a continuity-of-operations plan, to determine whether it will be restored as one of the agency's essential functions. CIAO officials stated that addressing critical assets in such plans is sufficient to meet the requirement for rapidly reconstituting minimum required capabilities, as long as these plans require reconstitution of the critical asset within 72 hours of its disruption. Although Project Matrix data do not indicate whether the plans meet the 72-hour criterion for a critical asset, they do show that for the three agencies with tentative critical assets, only 29 (58 percent) of the 50 assets identified were included in continuity-of-operations plans. Project Matrix data also showed that of those 29 included in the plans, 13 (45 percent) were over 2 years old. Although federal continuity-of-operations guidance does not specify how often plans should be updated, plans over 2 years old predate the terrorist attacks that occurred on September 11, 2001, and for Energy and EPA, predate the identification of their tentative critical assets. At least one agency, HHS, indicated that it is in the process of revising its continuity-of-operations plan, and it will ensure that all critical assets are included in its 72-hour recovery plan.

³⁴PDD 67, *Enduring Constitutional Government and Continuity of Government Operations*, issued October 21, 1998, required federal agencies to develop continuity of operations plans for essential operations. According to guidance issued by the Federal Emergency Management Agency (Federal Preparedness Circular 65, July 26, 1999), these plans are to provide for continued performance of essential federal functions under all circumstances.

Table 5: Critical Assets Included in Agencies' Continuity-of-Operations/Continuity-of-Government Plans as of December 2002

| Metric | HHS | Energy | EPA |
|---|---------|---------|-----------|
| Total number of critical assets tentatively identified | 18 | 14 | 18 |
| Continuity-of-operations/continuity-of-government plans | | | |
| Critical asset included | 9 (50%) | 2 (14%) | 18 (100%) |
| Number of those with tentatively identified critical asset included that are 2 years old or older | 2 (22) | 0 (0) | 11 (61) |

Source: Department of Health and Human Services, Department of Energy, Environmental Protection Agency (data), GAO (analysis).

ISACs' Progress in Implementing PDD 63-Suggested Activities Is Mixed

In addition to specific requirements for federal agencies, PDD 63 encouraged the voluntary creation of ISACs and suggested other activities for them to undertake in order to effectively gather, analyze, and disseminate information to and from infrastructure sectors and the federal government. The five ISACs we reviewed have the same basic operations, but all have different characteristics. For example, these voluntary ISACs were established at different times, and they had different funding sources and operational methods. In addition, their progress varies in terms of industry participation levels and the extent to which they have undertaken activities suggested by PDD 63.

Establishment and Operation of ISACs Differs

PDD 63 suggested that ISACs could serve as the mechanism for (1) gathering, analyzing, and appropriately sanitizing and disseminating private-sector information to both industry and NIPC and (2) gathering and analyzing information from NIPC for further distribution to the private sector. Further, the directive encouraged the voluntary creation of ISACs and left their actual design and functions, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. As a result, the five ISACs we reviewed were established differently and with membership open to a wide variety of organizations, according to the specific industry sector. The following brief overview of each ISAC illustrates their variations:

- The Information Technology ISAC is managed as a limited liability corporation; membership is open to companies that are engaged in the

information technology industry or that use the Internet for a major part of their business. Members can include vendors, manufacturers, or providers of Internet and E-commerce products (both hardware and software) and information technology solutions and services.

- The Telecommunications Infrastructure ISAC was established not as a separate entity but as a function of the National Coordinating Center for Telecommunications—a government-industry operational and collaborative body housed within the National Communications System. The National Communications System is being transferred to the new Department of Homeland Security, which is now the designated sector liaison. Membership is open to companies that provide telecommunications or network services, equipment, or software to the communications and information sector; select, competitive local exchange carriers; Internet service providers; vendors; software providers; telecommunications professional organizations and associations; or companies with participation or presence in the communications and information sector. Membership is also allowed for National Coordinating Center member federal departments and agencies, and for national security/emergency preparedness users.
- The Energy ISAC was originally managed as a limited liability corporation, but in late 2002 it changed its corporate structure to a tax-exempt organization. Its member companies are primarily in the oil and natural gas industries, and their activities include the exploration, production, processing, transmission, distribution, transportation, storage, trading, supervisory control and data acquisition, and E-commerce of energy commodities.
- The Electricity ISAC is managed and operated by the North American Electric Reliability Council, a nonprofit corporation that promotes electric system reliability and security. Its membership includes small and large electric utilities, regional utility companies, power marketers, and other entities responsible for power generation, transmission, control, and marketing and distribution in the United States, Canada, and a portion of Mexico.
- For the water sector, the Association of Metropolitan Water Agencies, a nonprofit corporation, is currently serving as the interim ISAC. Membership is open to drinking water and wastewater utilities, regardless of size.

The basic purpose of these ISACs' operations is the same: to facilitate information sharing among members by collecting, analyzing, and disseminating information on vulnerabilities, threats, intrusions, and anomalies reported by members, the government, and other sources, in order to avert or mitigate the impact of these factors. Also, all five reported that they provide some level of watch services 24 hours a day, 7 days a week.

Despite the overall similarities, these organizations differ in several ways. For example, existing organizations performed functions for some sectors many years before being designated as ISACs. The National Coordinating Center for Telecommunications performed some operations for the telecommunications sector beginning in 1984, and was designated an ISAC in January 2000. Similarly, before being designated for the electricity sector in October 2000, the North American Electric Reliability Council had been performing similar operations since 1968. In contrast, the Information Technology ISAC initiated operations in December 2000 in direct response to PDD 63. Further, although ISACs for Energy and Water were under consideration in response to PDD 63, they did not initiate operations until after September 11, 2001.

Industry participation reported by the ISACs—important to ensuring that incident and threat information is gathered and disseminated sectorwide—also varies. All the ISACs reviewed reported that they represent a majority of their respective industries, with highest representation reported by Information Technology (85 to 90 percent of the assets of Internet equipment and security providers by market share) and Telecommunications (over 90 percent of wire line telecommunications service providers by revenue market share, as well as a significant representation of wireless or Internet service and Internet backbone providers). The Energy ISAC reported that it represents 60 to 70 percent of the assets of the oil and gas industry, and the Electricity ISAC reported that it represents approximately 80 percent of the sector, including large and small utilities, regional utilities, and power marketers. The Water ISAC reported that it represents utilities that are serving 80 percent of drinking water and wastewater customers.

Table 6 summarizes basic information on each of the five ISACs reviewed, including when they began operations and their representation.

Table 6: Overview of Selected Information Sharing and Analysis Centers

| ISAC | Lead agency | Date operations began | Representation |
|------------------------|---|----------------------------|---|
| Telecommunications | Department of Commerce, through the National Communications System ^a | Some operations since 1984 | 90% of wire line telecommunications service providers by revenue market share, and significant representation of wireless or Internet service and Internet backbone providers |
| Electricity | Department of Energy | Some operations since 1968 | Approximately 80% of sector, including large and small utilities and power marketers |
| Information Technology | Department of Commerce, through its National Telecommunications and Information Administration ^a | December 2000 | 85–90% of assets of Internet equipment and security providers by market share |
| Energy | Department of Energy | November 2001 | 60–70% of sector |
| Water | Environmental Protection Agency | October 2001 | Utilities that are serving 80% of drinking water and wastewater customers |

Source: ISACs.

^aThe new Department of Homeland Security is now the designated lead agency for this sector.

The methods used to fund start-up and operational costs also differ by ISAC. For example, start-up and operational funding for Telecommunications and Electricity are provided through their sponsoring organizations, the National Communications System and the North American Electric Reliability Council, respectively. On the other hand, individual sector companies donated start-up funding for the Information Technology ISACs, and operational funding comes from membership fees paid by members. For the Energy ISAC, industry associations provided start-up funding, and membership fees initially provided operational funding. However, this ISAC reported that in the fall of 2002, the Office of Energy Assurance in the Energy Department agreed to fund ISAC operations—an agreement sought so that membership costs would not prevent smaller companies from joining. The new, cost-free Energy ISAC began operations and broad industry solicitation for membership in February 2003. For Water, a private-sector association provided start-up and initial operational funding, and the EPA also provided a grant for system development and expanded operations.

The ISACs reported differences in their management and operations. Although Telecommunications and Electricity were both developed as part

of preexisting sector activities, Telecommunications is housed in the National Communications System (a government entity), with private contractors performing operations co-located and procedurally integrated with government operations staff and industry representatives, and Electricity is part of the private-sector North American Electric Reliability Council, with its operations performed in-house. The Information Technology ISAC is a limited liability corporation, created specifically to oversee its operations, which are performed by a private contractor. Originally created as a limited liability corporation, the Energy ISAC reported that it changed its corporate structure to a tax-exempt organization to better facilitate and manage the funds provided by the Energy Department. And finally, the private-sector Association of Metropolitan Water Agencies initially performed operations in-house for Water. However, according to an ISAC official, in January 2003 a contractor began to perform operations, and subscribers are currently being actively recruited. Table 7 summarizes the entities that manage and operate each of the ISACs.

Table 7: Entities that Manage and Operate Selected Information Sharing and Analysis Centers

| ISAC | Management entity | Operational entity |
|------------------------|---|--|
| Telecommunications | National Communications System | Contracted watch and analysis operation co-located and integrated with government operational staff and industry |
| Electricity | North American Electric Reliability Council | Operated in-house by the North American Electric Reliability Council |
| Information Technology | Limited liability corporation | Contracted out to Internet Security Systems |
| Energy | Tax-exempt organization | Contracted out to Predictive Systems, Inc. |
| Water | Association of Metropolitan Water Agencies | Initially operated in-house, but contractor operations began in January 2003 |

Source: ISACs.

Progress for Suggested ISAC Activities Is Mixed

PDD 63 suggested several key ISAC activities to effectively gather, analyze, and disseminate information—activities that could improve the security posture of the individual sectors, as well as provide an improved level of communication within and across sectors and all levels of government. These are as follows:

-
- *Establishing baseline statistics and patterns on the various infrastructures.* This includes developing a database on the normal levels of computer security incidents that would be used for analysis purposes, to provide early indications of cyber attacks.
 - *Serving as a clearinghouse for information within and among the various sectors.* This includes disseminating information technology security information received from NIPC and members—such as incident reports and warnings, as well as ways to prevent or recover from them—to other ISACs.
 - *Providing a library of historical data for use by the private sector and government.* This includes collecting and posting information such as incident reports and warnings, references, vulnerability assessments, and related documents that can be accessed by all industry and government partners with a “need to know” for CIP.
 - *Reporting private-sector incidents to NIPC.* This includes reporting to NIPC security incidents that members authorize for reporting, and using standard operating procedures that contain guidelines on the event types and thresholds to report.

The ISACs showed mixed progress in implementing these activities, and none had completed all of them. By not fully implementing all these key activities, the ability of the ISACs to gather, analyze, and disseminate information within and across sectors and the government could be limited. Specifically, four of the five reported that efforts to establish baseline statistics were still in progress. Also, although three of the five reported that they serve as the clearinghouse for their own sector and also coordinate with other sectors, the remaining two reported that they serve as the clearinghouse for their own sector but are not coordinating with other sectors. Only one ISAC reported that it provides a library of incidents and historical data that is available to both the private sector and the federal government. Three reported that although they maintain such a library, it is available only to the private sector because of concerns that, if made available to the government, the information could be released under the Freedom of Information Act (FOIA).³⁵ The remaining ISAC reported that it has yet to develop a library, but plans to do so. Finally, officials for

³⁵Generally, FOIA (5 U.S.C. § 552) provides persons with the right of access to a broad range of federal agency records.

the Telecommunications, Information Technology, Electricity, and Water ISACs stated that they report incidents to NIPC on a regular basis and estimated that they report one to four incidents per month. According to NIPC officials, this volume of reporting may be appropriate for these particular ISACs, given established reporting thresholds, and other sources do not indicate that incidents are going unreported. In addition to formal incident reporting, the Information Technology ISAC reports that it and several other ISACs conduct daily information exchanges with the NIPC on current vulnerabilities, viruses, and attacks that affect cyber security. In contrast, officials for the Energy ISAC said that they have not reported to the government because of FOIA and antitrust concerns. Table 8 summarizes the reported status of the five ISACs in performing the activities suggested by PDD 63.

Table 8: ISACs' Progress in Performing Activities Suggested by PDD 63

| Activity | ISAC | | | | |
|--|--------------------|-------------|----------------------------------|----------------------------------|----------------------------------|
| | Telecommunications | Electricity | Information Technology | Energy | Water |
| Establish baseline statistics | In progress | In progress | Yes | In progress | In progress |
| Serve as clearinghouse within and among sectors | Yes | Yes | Yes | Only within own sector | Only within own sector |
| Provide library to private sector and government | In progress | Yes | Available only to private sector | Available only to private sector | Available only to private sector |
| Report incidents to NIPC | Yes | Yes | Yes | No | Yes |

Source: ISACs.

Efforts to Improve Cooperation and Interaction with ISACs and Assistance to Agencies Continue

NIPC continues to provide a number of information products to share warning information and to take actions to improve cooperation and interaction with the ISACs. Federal lead agencies have also assisted in ISAC establishment and operation. Citing some early problems in assistance and cooperation that have largely been overcome, ISACs identified areas in which efforts could be improved, such as receiving additional and more timely warnings. CIAO continues to assist federal agencies in using the Project Matrix methodology to identify critical assets and their dependencies.

NIPC and Agency Efforts to Improve Cooperation and Interaction with ISACs

As part of its overall responsibility to serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity, PDD 63 requires NIPC to provide a national focal point for gathering and disseminating information on threats to critical infrastructures, to establish its own relations with the ISACs, to provide them with sanitized or unsanitized reports, and to issue warning products in response to increases in threat condition. In addition, the lead agencies that PDD 63 designated for each critical infrastructure sector were also required to work with sector representatives in addressing problems related to CIP, including the creation of a private-sector ISAC.

To meet PDD 63 requirements to provide a national focal point and to disseminate threat and warning information, NIPC issues a variety of information products with three levels of infrastructure warnings—assessments, advisories, and alerts—that are developed and distributed as consistent with the FBI’s National Threat Warning System. *Assessments* address broad, general incident or issue awareness information and analysis that are significant and current, but they do not necessarily suggest immediate action. *Advisories* address significant threat or incident information that suggests a change in readiness posture, protective options, or response. *Alerts* address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures. These warning products have concentrated on cyber threats to critical infrastructures. And although these warnings will often be based on classified material and will include dissemination restrictions, NIPC usually publishes them in an unclassified format that reaches national security and civilian government agency officials, as well as infrastructure owners.

Over the past year, the NIPC has developed two additional types of warning products that address physical threats to critical infrastructures. *Information Bulletins* communicate issues that pertain to all or many of the critical infrastructures and are disseminated for informational purposes only. These bulletins are sent directly to the ISACs, as well as posted on NIPC’s public Web site. *Sector Notifications* communicate sensitive and developing information relating to one or more of the nation’s critical infrastructures. The notifications are sent to the ISACs for those infrastructures and are not publicly posted.

In his July 2002 congressional testimony, the NIPC director stated that since inception, NIPC has issued over 120 warning products, and that a number of these have preceded incidents or prevented them entirely by

alerting the user community to a new vulnerability or hacker exploit before acts are committed or exploits are used on a widespread basis. In addition, information on NIPC's Web site shows that it has issued 2 threat assessments, 11 advisories, and 3 alerts for calendar year 2002. These warnings concerned threats ranging from computer viruses and worms to a warning of potential cyber protests and potential system vulnerabilities, such as within the Simple Network Management Protocol (a protocol used by routers, switches, and hubs on the Internet and other related equipment). In addition, the NIPC has issued 11 Information Bulletins and 5 Sector Notifications during this period.

Other NIPC information products apprise policymakers and decisionmakers of current events, incidents, developments, and trends related to CIP. These products include its biweekly *CyberNotes*, which provides security and information system professionals with information on cyber vulnerabilities, hackers, viruses, and other critical infrastructure-related best practices, and, until recently, its monthly *Highlights*. In addition, in November 2002, NIPC also issued a white paper, *Risk Management: An Essential Guide to Protecting Critical Assets*, to assist security specialists and asset stakeholders in assessing physical and cyber risks to their organizations' critical assets.

In addition to information products, the FBI and NIPC lead and facilitate the InfraGard Program—an information-sharing and analysis effort that provides a mechanism for the public and private sectors to exchange information pertaining to cyber intrusion matters, computer network vulnerabilities, and physical threats on infrastructures. Under this program, private-sector members and FBI field representatives form local area chapters. InfraGard members, who currently total over 6,700, include state and local law enforcement agencies, other government entities, private industry, and academia. Actions to facilitate this program include gathering information and distributing it to members, educating the public and members on infrastructure protection, and disseminating information through the InfraGard network.

In discussing NIPC's sharing of warning information with the ISACs, two ISACs suggested that NIPC provide more warnings and alerts and two suggested that it provide more timely warnings. One also suggested that NIPC issue more detailed warnings that provide additional bases for action. The Information Technology ISAC suggested that NIPC further streamline the number of cyber threat warning levels, which can be confusing to industry. Further, it stated that NIPC's alerts represent the sum total input

from ISACs and other sources and, thus, often repeat ISAC information, usually in a less timely manner than did the original reports. This ISAC suggested that in addition to defining the government's specific information requirements, NIPC could add real value by publishing timely aggregate reports that include analyses not available elsewhere.

NIPC officials said that they are working to address some of these issues and reported that efforts are under way to educate the ISACs and the industries on the importance of submitting incident information, which could result in additional warnings. These officials also stated that their review procedures for issuing physical threat warnings are being streamlined and that they expect both the process and the timeliness to improve. In addition, these officials acknowledged that some threat alerts are at a general level and do not indicate what action should be taken, but they added that NIPC began issuing more high-level alerts in direct response to industry requests for high-level information that might indicate future attacks, such as those experienced on September 11th.

Regarding the requirement to establish its own relationship with the ISACs, in April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships, but that NIPC had undertaken a range of initiatives to foster information-sharing relationships with ISACs, as well as with government and international entities.³⁶ We recommended that it formalize these relationships and develop a plan to foster a two-way exchange of information between NIPC and the ISACs. In response to our recommendations, NIPC officials stated that in the summer of 2001 a new ISAC development and support unit had been created whose mission is to enhance private-sector cooperation and trust, resulting in a two-way sharing of information. Currently, 12 ISACs in total have been formed, and NIPC officials reported that the center has signed information-sharing agreements with most of these, including all but one of those we reviewed: the Energy ISAC. These officials added that most of the agreements contained industry-specific thresholds for cyber and physical incident reporting. Consistent with those sharing agreements, a number of ISACs currently transmit incident reports directly to NIPC, including the Energy ISAC and its members, which, according to an ISAC

³⁶U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

official, transmit incident reports via its secure CIP information system, InfraGard, or other means.

Federal lead agencies for the industry sectors covered by our review also noted efforts to develop relationships and encourage information-sharing and partnering with the ISACs. For example, the Department of Energy reports that it maintains daily contact with officials from both the Energy and the Electricity ISACs, to exchange appropriate sensitive information. Further, in order to share appropriate classified threat information, the department reports that its Office of Energy Assurance has obtained clearances for more than 300 persons, including staff for both ISACs as well as officials of various oil, natural gas, and electric power firms.³⁷ This office also works closely with NIPC and the National Joint Terrorism Task Force. As another example, Commerce's NTIA reports that since the release of PDD 63 in 1998, its Communications and Information Infrastructure Assurance Program has focused on working closely with the private sector to develop and implement a vulnerability awareness and education program for the information and communications sector, to facilitate industry-government cooperation on CIP research and development, and to support a growing CIP international outreach program.

Concerning the support provided by their lead agencies, officials representing four of these ISACs—Telecommunications, Information Technology, Water, and Electricity—said that they had good working relationships with their lead agencies. For example, Electricity stated that it has an excellent relationship with the Department of Energy. In contrast, the Energy ISAC expressed concerns with the Department of Energy's lack of clear support in creating the ISAC and with the high turnover in the agency liaison position. The other lead agencies—the National Communications System, Commerce, and EPA—all reported good working relationships with their ISACs. The Department of Energy reported that it is taking steps to improve the current information-sharing process, which included assigning three additional analysts from its Office of Energy Assurance to support NIPC.

³⁷The Office of Energy Assurance and its functions are to transition to the Department of Homeland Security.

CIAO's Agency Assistance Focuses on Project Matrix

According to PDD 63, the CIAO is required to coordinate analyses of the federal government's own dependencies on critical infrastructures. As discussed previously, to assist the agencies in protecting their own critical assets, this office has provided guidance, including its *Vulnerability Assessment Framework* and its *Practices for Securing Critical Information Assets*. In addition, in March 2000 it began assisting the agencies in implementing its Project Matrix methodology to identify their critical assets and these assets' dependencies on other government assets and private-sector infrastructures—assistance the agencies we reviewed agreed was needed to help them identify assets of national importance.

Currently, CIAO provides assistance in applying Project Matrix in the form of teams that help the agencies conduct step 1 of the methodology and plans to assist in conducting Project Matrix step 2 analyses for two assets at each agency. In addition, as mentioned previously, CIAO is also currently revising and streamlining its Project Matrix methodology to consolidate some steps and make it less labor intensive for the agencies.

PDD 63 Implementation Presents Challenges and Obstacles

The agencies and organizations identified challenges and obstacles that could adversely affect their efforts to protect their critical infrastructures. These challenges and obstacles are primarily ensuring adequate CIP resources, coordinating security activities for agencies' critical assets, and having ISACs share information with the federal government.

Agencies Report Challenges in Justifying CIP Resources

All the agencies we reviewed have received increased CIP funding in recent years. However, they also noted that there will be continuing challenges to obtain the funding needed to protect their critical assets.

Like many agencies, the four we reviewed do not receive appropriations specifically designated for CIP, but do collect information and data on their CIP programs and report them to OMB as part of its national security crosscut data call, from which it prepares its annual report to the Congress on combating terrorism. OMB's October 2001 guidance to the agencies for the national security crosscut contains detailed instructions on identifying and categorizing CIP activities, including identifying agency systems that are mission critical on a national level, not just an agency level; designating whether activities pertain to internal agency critical infrastructures or to the critical infrastructure sectors identified in PDD 63; and identifying

specific critical infrastructure program areas, such as threat/vulnerability/risk assessments and education and training. In addition, the guidance gave instructions for allocating activities among multiple sectors and distinguishing between cyber and physical activities. It also recognized potential overlap with data reported for other portions of the data call, such as a physical security activity being counted as part of both the CIP and combating terrorism data.

Although there are differences in the way these four agencies report their CIP spending, the data they reported to OMB for its June 2002 report showed significant overall increases in CIP funding for fiscal years 2002 and 2003 as compared with fiscal year 2001.³⁸ These data are summarized in table 9.

Table 9: Critical Infrastructure Spending by the Departments of Commerce, Energy, and Health and Human Services and the Environmental Protection Agency (Fiscal Years 2001–2003, Dollars in Millions)

| Agency | Fiscal year 2001 (actual) | Fiscal year 2002 (enacted) | Fiscal year 2002 supplemental (enacted) | Fiscal year 2003 (budget) |
|-----------------------|------------------------------|-------------------------------|---|------------------------------|
| Commerce ^a | \$27.9 | \$30.1 | \$10.3 | \$50.7 |
| Energy | 48.4 | 46.3 | 0.0 | 71.8 |
| EPA | 2.2 | 3.4 | 121.0 | 41.7 |
| HHS | 84.3 | 96.8 | 0.0 | 87.2 |
| Total | \$162.8 | \$176.5 | \$131.3 | \$251.3 |

Source: OMB's *Annual Report to Congress on Combating Terrorism*, June 2002.

Note: Totals may not add because of rounding, and we did not validate the accuracy of reported amounts.

^aIncludes funding to support operations of Commerce's National CIAO.

As this table shows, CIP funding for these four agencies increased from \$162.8 million in fiscal year 2001 to \$176.5 million in fiscal year 2002 (an increase of \$13.7 million, or 8 percent). An emergency response supplemental appropriation in 2002 following the September 11, 2001, attacks added an additional \$131.3 million, of which \$119 million was for EPA to provide additional physical security for its facilities and to assist

³⁸Office of Management and Budget, *Annual Report to Congress on Combating Terrorism* (June 2002).

utilities in conducting vulnerability assessments for large drinking water systems. Including the supplemental, spending enacted for fiscal year 2002 totaled \$307.8 million—an increase of \$145.0 million, or 89 percent, compared with fiscal year 2001. For fiscal year 2003, CIP funding for the four agencies totaled \$251.3 million—\$56.5 million less than the total for fiscal year 2002 and the supplemental, but still an increase of \$88.5 million, or 54 percent, compared with fiscal year 2001.

Although most of the agencies we reviewed received significant additional CIP appropriations for fiscal years 2002 and 2003, agencies noted the following examples of challenges in obtaining CIP funding:

- In June 2001, the EPA IG reported that the agency's participation in Project Matrix had been delayed since February 2001 because of insufficient funding. Further, the OIG reported that OMB denied without comment EPA's fiscal year 2001 request for \$5 million for physical measures under PDD 63.
- Officials in Commerce's Office of the CIO said that the department's fiscal year 2001 budget request included \$79 million to perform vulnerability assessments, mitigate vulnerabilities, and train employees. However, according to these officials, OMB denied the request because it was not based on completed vulnerability assessments and detailed remediation plans. Further, they said that the department's fiscal year 2002 budget request included amounts in each operating unit's budget to perform vulnerability assessments, with a plan to request the mitigation funding in fiscal year 2003. However, the department denied the requested funding for the planned assessments and for virtually all the mitigation efforts because, according to a Commerce Office of Budget official, OMB guidance directed that only requests for current service levels could be submitted.

-
- Officials in Energy's Office of Security stated that OMB had denied \$16 million for security that the department had requested as part of a fiscal year 2002 supplemental. In a March 28, 2002, letter to OMB, the Director of Energy's Office of Management, Budget, and Evaluation/Chief Financial Officer said that the denial of this request had left the department with inadequate funds to implement security measures that would appropriately respond to the terrorist attacks of September 11, 2001. According to this letter, OMB denied the supplemental security proposals because of the pending revision of Energy's Design Basis Threat, a document that outlines the basis for physical security measures.³⁹

Resources will be needed for the agencies to complete their Project Matrix efforts and for other CIP activities related to their critical assets, including conducting and updating vulnerability assessments, correcting identified vulnerabilities, and preparing and updating continuity of operations plans. In part, the Project Matrix reviews themselves may help the agencies prioritize and justify their CIP spending. OMB is requiring all large agencies to undergo a Project Matrix review to more clearly identify and prioritize the security needs for government assets. In addition, OMB identifies these reviews as a key element in its efforts to identify the critical operations and assets of the federal government's critical enterprise architecture and to better prioritize and fund the government's security needs.

Agencies Face Challenges Coordinating CIP Efforts

With responsibilities for the security of cyber and physical assets assigned to the CIOs and chief infrastructure assurance officers, respectively, and to separate agency organizations, several of the agencies noted challenges in coordinating efforts internally to identify and protect their critical assets. In addition, we identified a challenge in coordinating critical asset protection with GSA, which provides protective services for many agencies' facilities or buildings.

³⁹The Design Basis Threat for the Department of Energy identifies and characterizes potential adversary threats to its programs and facilities in order to protect against activities including unauthorized access; theft, diversion, or loss of control of nuclear weapons, weapons components, special nuclear material, associated technologies and hardware, and critical technologies; sabotage; espionage; loss or theft of classified material or government property; and other acts that may cause unacceptable adverse impacts on national security, the health and safety of employees, the public, or the environment. Among other things, the Design Basis Threat is used to develop safeguards and security programs and requirements and to provide a basis for site safeguards and security program planning, implementation, and facility design.

As discussed previously, three of the four agencies had security responsibilities for cyber assets assigned to the CIO, with responsibilities for physical assets assigned to a separate chief infrastructure assurance officer in another organization. For example, at EPA, the Office of Environmental Information, which houses the agency's CIO, was responsible for cyber security, and the Office of Administration and Resources Management was responsible for physical security. At Commerce, as permitted by PDD 63, the CIO was also designated the chief infrastructure assurance officer and, thus, was responsible for both cyber and physical assets; the department also maintained a separate office of security that was responsible for physical security.

Officials at the agencies noted varying levels of coordination between the organizations responsible for cyber and physical security, including coordination on an as-needed basis, with no formal process at EPA; a formal memorandum of agreement on the review of cybersystems at Commerce; and weekly cyber security coordination meetings held at Energy with representatives from the Office of the CIO, the Office of Security, the Office of Independent Oversight and Performance Assurance, and the IG. Despite these coordination mechanisms, their efforts to identify and protect their critical assets highlighted coordination challenges that the agencies are addressing. For example, our initial discussions with an official in Commerce's Office of Security indicated that coordination of security matters between that office and the office of the CIO was a problematic and ongoing issue. However, the Director of Security, who was appointed in August 2002, and the CIO office's Information Technology Security Program Manager report that these offices are now working to establish an integrated approach to security matters, including CIP and continuity-of-operations planning. As another example, for critical assets at HHS, there were inconsistencies between the physical vulnerability assessment dates maintained by the CIO's office and those maintained by the office responsible for physical security—discrepancies that were not identified until prompted by our request for updated data.

Our analyses also identified an external coordination challenge with GSA, which may often be responsible for protecting agency facilities or buildings that house critical assets. According to GSA officials, they are not aware of whether a critical asset is in one of the facilities they manage unless the agency specifically shares that information—something GSA expects the agencies to do during GSA's vulnerability assessment process. However, this information is not always shared, and in one instance HHS officials confirmed that GSA had not been informed that an HHS critical asset was

housed within a GSA-owned building. GSA officials agreed that knowing whether facilities or their assets are considered critical could affect the level of security it provides, and it also indicated that this may be something that GSA should routinely inquire about as part of its vulnerability assessment process.

ISACs Face Information-Sharing Challenges

Officials for the five ISACs we contacted noted numerous challenges that could affect their establishment and operation, but they most often identified FOIA as a major challenge that hinders the sharing of intelligence and incident information between infrastructure sectors and the federal government. Two ISACs also identified sharing information among industry partners as a challenge because such cooperation could open companies to prosecution under antitrust regulations. Options being considered and actions taken to help overcome these challenges include restrictions on government use and disclosure of critical infrastructure information, such as those included in the recently enacted Homeland Security Act of 2002, as well as the use of public policy tools to provide incentives.

The range of challenges identified by the ISACs included convincing businesses of their value and benefit; overcoming members' mistrust of government; not having a standard model to follow; setting up a limited liability corporation; finding a contractor with the proper information technology security controls to ensure that data are protected; obtaining security clearances to enable the sharing of classified information with ISAC staff who have a "need to know," and ensuring secure communications for sharing this information; and providing for communication outside of the public switched network, such as satellite phones. In addition, according to the Telecommunications Infrastructure ISAC, the chief concern of its members is the issue of liability associated with reporting a problem involving another company. Such challenges may affect member participation and the amounts of information shared by both the members and the government. For one challenge in particular—providing security clearances—officials for NIPC stated that NIPC is taking actions to expedite clearances, and its goal is to establish security clearances to one or two members of the managing board for each ISAC. An official for the Electricity ISAC noted that security clearances have been provided to several subject matter experts in the sector, but he also stressed the importance of ensuring secure communications for those holding clearances either through the ISAC itself or through access to federal secure communications facilities.

One challenge reported by all five ISACs, however, was the concern about reporting incident information that could be subject to FOIA requests. In addition, two reported that their members are concerned about the risk of prosecution under antitrust regulations for sharing information with other industry partners—a concern also acknowledged in the *National Strategy for Homeland Security* and by NIPC in a July 2002 congressional testimony.⁴⁰ As mentioned previously, an Energy ISAC official stated that it does not plan to share information with the federal government until these issues are resolved, and some ISAC officials suggested that existing FOIA and antitrust legislation be modified to provide specific exemptions for reported incident information.

The July 2002 *National Strategy for Homeland Security* includes “enabling critical infrastructure information sharing” among 12 major legislative initiatives it outlines and states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate its voluntary submission. This strategy states that the Attorney General will convene a panel to propose any legal changes necessary to enable the sharing of essential homeland security–related information between the federal government and the private sector. In addition, we have testified on the continuing debate concerning the protections provided to private-sector entities as they are encouraged to disclose and exchange information on both physical and cyber security problems and solutions that are essential to protecting our nation’s critical infrastructures.⁴¹

In response to some of these concerns, the Congress included provisions in the Homeland Security Act of 2002 that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to the Department of Homeland Security. These restrictions include an exemption from disclosure under FOIA, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties

⁴⁰Testimony of Ronald Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

⁴¹U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges Need to Be Addressed*, [GAO-02-961T](#) (Washington, D.C.: July 24, 2002).

for any federal employee who improperly discloses any protected critical infrastructure information. At this time, it is too early to tell what impact the new law will have on the willingness of the private sector to share critical infrastructure information.

In addition to legislation, public policy tools have also been discussed and used as another approach to encouraging increased private-sector CIP efforts and information sharing with the federal government. In his June 2002 testimony on the then-proposed Department of Homeland Security, the Comptroller General noted that intelligence and information-sharing challenges highlight the need for strong partnerships with those outside the federal government, and that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.⁴² Further, the *National Strategy for Homeland Security* discusses the need to use available policy tools to raise the security of our critical infrastructures, and it specifically mentions federal grants programs to assist state and local efforts and legislation to create incentives for the private sector. Public policy tools available to governments include grants, regulations, tax incentives, and regional coordination and partnerships, and some of these are already being used. For example, as the lead agency for the water sector, EPA reported providing 449 grants totaling \$51 million to assist utilities for large drinking water systems in preparing vulnerability assessments, emergency response/operating plans, security enhancement plans and designs, or a combination of these efforts. In a different approach, the American Chemistry Council, the ISAC for the chemical sector, requires that as a condition of membership, its members perform enhanced security activities, including vulnerability assessments.

Conclusions

Although recent executive orders and national strategies reemphasize the importance of CIP, efforts to fully implement PDD 63 requirements for protecting agencies' critical assets and enhancing information sharing through voluntary private-sector ISACs are not quickly achieving the results necessary to protect major sectors of our nation's critical infrastructure in a post-September 11th environment. The agencies have made progress in implementing PDD 63 requirements, and most have

⁴²U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success*, [GAO-02-886T](#) (Washington, D.C.: June 25, 2002).

tentatively identified or are revisiting their list of critical assets. Further, CIAO is currently undertaking efforts to streamline its Project Matrix methodology. However, with no established agency or government milestones and with resource uncertainties, it is difficult to estimate when the agencies will complete the process of identifying their critical assets and dependencies. This difficulty also creates uncertainties as to when other key steps in protecting critical assets will be completed—steps that are not routinely tracked from both a cyber and physical perspective for critical assets, such as identifying their vulnerabilities, developing remediation plans, and developing plans to ensure the continuity of critical operations. Other agencies, such as GSA, are also a critical element in this process to ensure that once critical assets are identified, appropriate security is provided for the facilities and buildings that house them. Further, identifying critical assets and taking the other key steps needed to protect them can help the agencies identify and obtain required resources. Until these processes and steps are completed, neither the agencies nor the federal government can ensure that the operations and infrastructures essential to national security, national economic security, and national public health and safety are safeguarded against attack and could be rapidly reconstituted if a successful infrastructure attack or disruption were to occur.

The five ISACs have made progress in establishing ISAC operations. However, mixed progress in suggested activities and other challenges and obstacles they reported potentially limit their ability to gather incident information and disseminate it between their industry sectors and the federal government. This potential limitation could affect NIPC's efforts to provide timely warning information for the government and other industry sectors. NIPC and the lead agencies continue to work with the ISACs to improve the public/private partnership called for by PDD 63 and subsequent federal plans and strategies. The Homeland Security Act of 2002, in part, responds to the ISACs' FOIA concern by including information use and disclosure restrictions. However, it remains to be seen whether these efforts will result in increased information sharing with the federal government and whether additional federal actions, such as the use of public policy tools, could offer potential incentives to encourage increased private-sector CIP efforts.

Given what we found for these selected agencies and ISACs, we believe that it is crucial that the administration also know the status and progress of CIP activities for all major federal agencies and critical infrastructure sectors.

Recommendations for Executive Action

To (1) help ensure the identification and adequate protection of critical agency cyber-based and physical assets and (2) reinforce management's commitment to prioritize the protection of critical infrastructure throughout agencies, we recommend that the Secretaries of Commerce, Energy, and Health and Human Services and the Administrator of the Environmental Protection Agency all direct their respective CIOs and chief infrastructure assurance officers to work together, as appropriate, to:

- coordinate with CIAO to set milestones to complete their Project Matrix analyses that will identify each agency's critical cyber, physical, and other assets and the dependencies of these assets on other government operations and privately owned critical infrastructures;
- require, concurrently with the identification of critical assets and their dependencies, that vulnerability assessments be conducted or updated where warranted, to appropriately consider (1) the specific assets identified as critical national assets and their dependencies, (2) both cyber and physical vulnerabilities of these assets, and (3) changes in the threat environment, particularly as reflected by recent terrorist activity and in warnings by the Office of Homeland Security and NIPC;
- ensure that remediation plans for correcting identified critical asset vulnerabilities are developed, specifying corrective actions and the time lines, responsibilities, and funding for their implementation; and that cyber-related actions are also reflected in the agency's information security corrective-action plans, and that updates are reported to OMB;
- ensure that agency continuity-of-operations plans are prepared or updated to incorporate critical assets and, according to the CIAO criterion, that they provide for the reconstitution of these assets within 72 hours of a successful infrastructure attack or disruption;
- routinely track and monitor the status of vulnerability assessments, corrective actions, and other security efforts related to critical assets, such as the development of continuity-of-operations plans; and provide an annual status update to help support budget requests and other reporting requirements, such as those of the Government Performance and Results Act and the Federal Information Security Management Act;

-
- formally apprise the General Services Administration when facilities or buildings for which it has protective responsibilities house agency-critical assets identified through the Project Matrix process; and
 - use Project Matrix plans and results to help prioritize and prepare budget justifications for resources needed to identify and protect the agency's own critical infrastructures.

To help ensure that private-sector ISACs continue efforts to improve their CIP activities, we recommend that the Secretary of Energy, the Secretary of Commerce, and the Administrator of the Environmental Protection Agency, through their lead agency responsibilities for the energy, electricity, information, communication, and water industry sectors, assess the need for grants, tax incentives, regulation, or other public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government. After lead agency responsibilities for the information and telecommunications sector are transitioned to the Department of Homeland Security, the Secretary of that department would become responsible for this recommendation for that sector.

To assist the administration in establishing CIP priorities for all major federal agencies, critical infrastructure sectors, and the Department of Homeland Security, we further recommend that

- the Director of the Critical Infrastructure Assurance Office determine the status of, and identify additional actions needed to improve the federal government's efforts and progress in implementing, federal CIP policy, including identifying the federal government's critical assets, completing vulnerability assessments for these assets, remedying identified vulnerabilities, and incorporating these assets into continuity of operations plans; and
- the Director of the National Infrastructure Protection Center determine the status and identify additional actions needed to improve the quality and quantity of information being provided by the ISACs, and of plans made by the new department's Information Analysis and Infrastructure Protection directorate and the ISACs to enhance the current information-sharing process.

These organizations should coordinate the implementation of these recommendations with the Department of Homeland Security, which is

responsible for developing the comprehensive national plan and will become responsible for the recommendations as the organizations transition to the department.

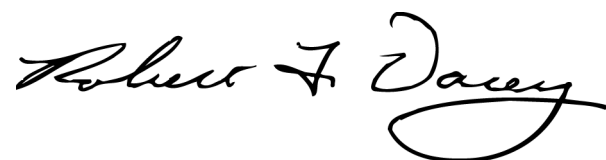
Agency Comments and Our Evaluation

The Inspector General for the Department of Health and Human Services transmitted the department's written comments on a draft of this report (see app. I). The department concurred with our recommendations for executive agencies and noted that, in many cases, it is already engaged in the recommended activities. Also, in responding to our recommendation that agencies ensure that their continuity-of-operations plans are prepared or updated to incorporate critical assets and provide for the reconstitution of these assets within 72 hours of a successful infrastructure attack or disruption, the department commented that its physical security officials will work closely with its Continuity of Operations Plan program to ensure that all critical assets are included in the 72-hour recovery plan. Regarding our recommendation that agencies formally apprise GSA when facilities or buildings for which it has protective responsibilities house agency-critical assets, the department commented that physical security officials would coordinate with GSA/Federal Protective Service on updating the list of CIP sites. We also received written and oral technical comments from the Department of Commerce's CIAO and its National Telecommunications and Information Administration, EPA, HHS, the FBI, the National Communications System, the North American Electric Reliability Council, the Association of Metropolitan Water Agencies, and the Energy and Information Technology ISACs. Comments from all these organizations have been incorporated into the report, as appropriate.

As agreed with your staff, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to other interested congressional committees and the heads of the agencies discussed in this report, as well as to the private-sector participants and other relevant agencies. In addition, 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 Ben Ritt, Assistant Director, at (202) 512-6443. We can also be reached by E-mail at dacey@ga.gov or

rittw@gao.gov, respectively. Staff who made key contributions to this report are listed in appendix II.

A handwritten signature in black ink that reads "Robert F. Dacey". The signature is written in a cursive style with a large, looping flourish at the end of the name.

Robert F. Dacey
Director, Information Security Issues

Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

JAN 27 2003

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

Dear Mr. Dacey:

Enclosed are the department's comments on your draft report entitled, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors." The comments represent the tentative position of the department and are subject to reevaluation when the final version of this report is received.

The department also provided several technical comments directly to your staff.

The department appreciates the opportunity to comment on this draft report before its publication.

Sincerely,

A handwritten signature in cursive script that reads "Janet Rehnquist".

Janet Rehnquist
Inspector General

Enclosure

The Office of Inspector General (OIG) is transmitting the department's response to this draft report in our capacity as the department's designated focal point and coordinator for General Accounting Office reports. The OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.

Appendix I
Comments from the Department of Health
and Human Services

Comments of the Department of Health and Human Services to the General Accounting Office's Draft Report, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors" (GAO-03-233)

General Comments

The Department of Health and Human Services (HHS) appreciates the opportunity to comment on this draft report.

GAO Recommendations for Executive Action

To (1) help ensure the identification and adequate protection of critical agency cyber-based and physical assets and (2) reinforce management's commitment to prioritize the protection of critical infrastructure throughout agencies, we recommend that the Secretaries of Commerce, Energy, Health and Human Services, and the Administrator of the Environmental Protection Agency each direct their CIOs and chief infrastructure assurance officers to work together, as appropriate, to:

- Coordinate with CIAO to set milestones to complete their Project Matrix analyses that will identify the agency's critical cyber, physical, and other assets; and the dependencies of these assets on other government operations and privately owned critical infrastructures
- Concurrent with the identification of critical assets and their dependencies, require that vulnerability assessments be conducted or updated where warranted to appropriately consider (1) the specific assets identified as critical national assets and their dependencies; (2) both cyber and physical vulnerabilities of these assets; and (3) changes in the threat environment, particularly as reflected by recent terrorist activity and in warnings by the Office of Homeland Security and NIPC
- Ensure that remediation plans for correcting identified critical asset vulnerabilities are developed, specifying corrective actions and the timelines, responsibilities, and funding for their implementation, and that those actions that are cyber-related are also reflected in the agency's information security corrective action plans and updates reported to OMB
- Ensure that agency continuity of operations plans are prepared or updated to incorporate critical assets and, according to CIAO criterion, provide for reconstitution of these assets within 72 hours of a successful infrastructure attack or disruption
- Routinely track and monitor the status of vulnerability assessments, corrective actions, and other security efforts related to critical assets, such as the development of continuity of operations plans; and provide an annual status update to help support budget requests and other reporting requirements, such as

Appendix I
Comments from the Department of Health
and Human Services

those of the Government Performance and Results Act and the Federal Information Security Management Act

- Formally apprise the General Services Administration when facilities or buildings for which it has protective responsibilities house agency critical assets identified through the Project Matrix process
- Use Project Matrix plans and results to help prioritize and prepare budget justifications for resources needed to identify and protect the agency's own critical infrastructures.

HHS Response

The HHS concurs with GAO's recommendations for executive agencies. In many cases, we already are engaged in the recommended activities.

In terms of our response to specific recommendations: GAO was concerned that HHS has not provided for immediate reconstitution of critical assets. The HHS Physical Security officials will work closely with the Continuity of Operations Plan program to ensure all critical assets are included in the 72 hours recovery plan. Also, GAO was concerned that HHS was not coordinating with the General Services Administration (GSA) on the identification of HHS critical assets that are housed in GSA buildings. The HHS Physical Security officials will coordinate with GSA/Federal Protective Service on updating the list of Critical Infrastructure Protection sites.

GAO Contact and Staff Acknowledgments

GAO Contact

William B. Ritt, (202) 512-6443

Acknowledgments

In addition to the person named above, Shirley Bates, Elena Epps, Joanne Fiorino, Sophia Harrison, Danielle Hollomon, Barbarol James, David Powner, Jamie Pressman, Jamelyn Smith, Jessica Steele, Cady Summers, Larry Turman, and Kathleen Turner made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and 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 GAO Mailing Lists" under "Order GAO Products" 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

**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**

