United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EDT
Tuesday, April 8, 2003

INFORMATION SECURITY

Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures

Statement of Robert F. Dacey
Director, Information Security Issues

April 8, 2003

INFORMATION SECURITY

Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures

GAO Highlights

Highlights of GAO-03-564T, a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Protecting the computer systems that support federal agencies' operations and our nation's critical infrastructures—such as power distribution, telecommunications, water supply, and national defense—is a continuing concern. These concerns are well-founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks. GAO first designated computer security as high risk in 1997, and in 2003 expanded this high-risk area to include protecting the systems that support our nation's critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP.

GAO has made previous recommendations and periodically testified on federal information security weaknesses—including agencies' progress in implementing key legislative provisions on information security—and the challenges that the nation faces in protecting our nation's critical infrastructures. GAO was asked to provide an update on the status of federal information security and CIP.

www.gao.gov/cgi-bin/getrpt?GAO-03-564T.

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

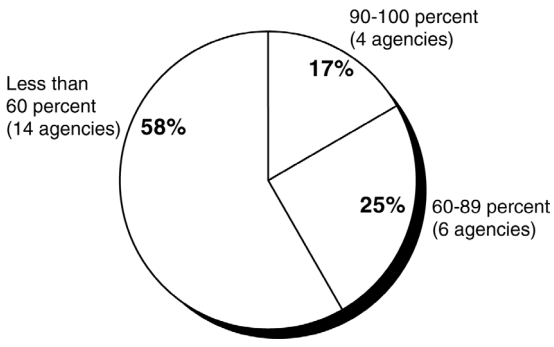
What GAO Found

With the enactment of the Federal Information Security Management Act of 2002, the Congress continued its efforts to improve federal information security by permanently authorizing and strengthening key information security requirements. The administration has also made progress through a number of efforts, among them the Office of Management and Budget's emphasis of information security in the budget process.

However, significant information security weaknesses at 24 major agencies continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. Although recent reporting by these agencies showed some improvements, GAO found that agencies still have not established information security programs consistent with the legal requirements. For example, periodic testing of security controls is essential to security program management, but for fiscal year 2002, 14 agencies reported they had tested the controls of less than 60 percent of their systems (see figure below). Further information security improvement efforts are also needed at the governmentwide level, and these efforts need to be guided by a comprehensive strategy in which roles and responsibilities are clearly delineated, appropriate guidance is given, adequate technical expertise is obtained, and sufficient agency information security resources are allocated. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address critical challenges that GAO has identified over the last several years. These challenges include

- developing a comprehensive and coordinated national CIP plan;
- improving information sharing on threats and vulnerabilities between the private sector and the federal government, as well as within the government itself;
- improving analysis and warning capabilities for both cyber and physical threats; and
- encouraging entities outside the federal government to increase their CIP efforts.

Percentage of systems with security controls tested during fiscal year 2002



Source: Agency-reported data.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the challenges that our nation faces concerning federal information security and critical infrastructure protection (CIP). Federal agencies and other public and private entities rely extensively on computerized systems and electronic data to support their missions. CIP involves activities that enhance the security of the cyber and physical public and private infrastructures that are essential to our national security, national economic security, and/or national public health and safety. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information. Further, protecting against computer-based attacks on critical infrastructures is an important aspect of homeland security.

The Congress has continued to hold important hearings and has passed legislation that the President has signed into law to strengthen information security practices throughout the federal government and to better address threats to the nation's critical computer-dependent infrastructures. Such legislation includes Government Information Security Reform provisions (commonly known as "GISRA"), which established information security program, evaluation, and reporting requirements for federal agencies;[1] the recently enacted Federal Information Security Management Act of 2002 ("FISMA"), which permanently authorized and strengthened GISRA;[2] and the Homeland Security Act of 2002, which, among other things, consolidated certain essential CIP functions and organizations in the Department of Homeland Security.

In my testimony today, I will provide an overview of the increasing nature of cyber security threats and vulnerabilities and of the continuing pervasive weaknesses that led GAO to initially begin reporting information security as a governmentwide high-risk issue in 1997. I will then discuss the status of actions taken by the Office of Management and Budget (OMB) to address overall weaknesses and challenges identified through its

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

[2]Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

GISRA analyses, as well as the federal government's continuing need to be guided by a comprehensive improvement strategy. I will also discuss the results of our evaluation of efforts by 24 of the largest federal agencies to implement the requirements of GISRA and to identify and correct their information security weaknesses.[3] Finally, I will discuss the federal government's evolving approach to and current strategies for protecting our nation's critical infrastructures. In this discussion, I will highlight the challenges, identified in prior GAO work that the nation continues to face in implementing CIP. These challenges include developing a comprehensive and coordinated national CIP plan, implementing better information sharing on threats and vulnerabilities, improving analysis and warning capabilities, and ensuring appropriate incentives to encourage nonfederal CIP efforts. In January 2003, GAO expanded its information security high-risk issue to include cyber CIP.[4]

As agreed, this testimony incorporates the preliminary results of our analyses of federal agencies' efforts to implement GISRA information security requirements during fiscal year 2002, which was originally requested by the chair and ranking minority member of a former subcommittee of the House Government Reform Committee. In conducting this review, we analyzed (1) executive summaries and reports that summarized management reviews by the 24 agencies for their information security programs, (2) inspector general (IG) summaries and reports on their independent evaluations of these agencies' programs, and (3) agency plans to correct their identified information security weaknesses. We did not validate the accuracy of the data provided in these summaries, reports, and plans. We also discussed with OMB officials the status of their actions and initiatives to improve and provide additional guidance for federal information security. We performed our work from September 2002 to April 2003 in accordance with generally accepted government auditing standards.

[3]These are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, the Environmental Protection Agency, Federal Emergency Management Agency, General Services Administration, Office of Personnel Management, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[4]U.S. General Accounting Office, *High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

Results in Brief

Protecting the computer systems that support our nation's critical operations and infrastructures is a continuing concern. Telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. Yet with this dependency comes an increasing concern about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. Such concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

With the enactment of FISMA, the Congress continued its efforts to improve federal information security by permanently authorizing and strengthening the information security program, evaluation, and reporting requirements established by GISRA. The administration has also made progress through a number of efforts, including OMB's emphasis of information security in the budget process and e-government initiatives and the National Institute of Standards and Technology's (NIST) issuance of additional computer security guidance. However, our recently reported analyses of audit and evaluation reports issued from October 2001 to October 2002 for 24 major agencies showed that significant information security weaknesses continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, all 24 agencies had weaknesses in security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. In addition, although our most recent analyses of fiscal year 2002 GISRA reporting by these agencies showed some improvements, agencies still have not established information security programs consistent with the requirements of GISRA. For example, although the percentage of systems assessed for risk increased for 13 agencies, for 9 agencies, less than 60 percent of their systems had risk assessments (an essential element of risk management and overall security program management that helps ensure that the greatest risks have been identified and addressed). Further, although 15 agencies reported increases in the number of systems for which controls had been tested and evaluated, 14 reported that controls had been tested for less than 60 percent of their systems.

As we have previously recommended, further information security improvement efforts are needed at the governmentwide level, and it is

important that these efforts are guided by a comprehensive strategy. As the development of this strategy continues, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of CIP; providing more specific guidance on the controls that agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Over the years, a variety of working groups has been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. Although the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, we have identified and made numerous recommendations over the last several years concerning critical infrastructure challenges that need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, even greater efforts are needed to address them. These challenges include the following:

- *Developing a comprehensive and coordinated national CIP plan.* A more complete plan is needed that will address specific roles, responsibilities, and relationships for all CIP entities; clearly define interim objectives and milestones; set time frames for achieving objectives; and establish performance measures.

- *Improving information sharing on threats and vulnerabilities.* Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber and physical attacks, which could threaten the national welfare. Information sharing needs to be enhanced both within the government and between the federal government and the private sector and state and local governments.

- *Improving analysis and warning capabilities.* More robust analysis and warning capabilities, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats.

- *Encouraging entities outside the federal government to increase their CIP efforts*. Although budget requests include funds (1) to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that our nation's critical infrastructures are adequately secured across all critical infrastructure sectors and (2) for outreach efforts to state and local government and the private sector, incentives will still be needed to encourage nonfederal entities to increase their CIP efforts. These incentives could include grants, regulations, tax incentives, and regional coordination and partnership.

It is also important that CIP efforts are appropriately integrated with the transition of certain CIP functions and entities to the new Department of Homeland Security (DHS).

Incidents, Threats, and Potential Attack Consequences are Significantly Increasing

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way 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, in addition to such benefits, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age on the other hand, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Table 1 summarizes the key threats to our nation's infrastructures, as observed by the Federal Bureau of Investigation (FBI).

Table 1: Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,[a] can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation unless otherwise indicated

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

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access

to data.[5] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology (IT), the likelihood increases that information attacks will threaten vital national interests.

As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

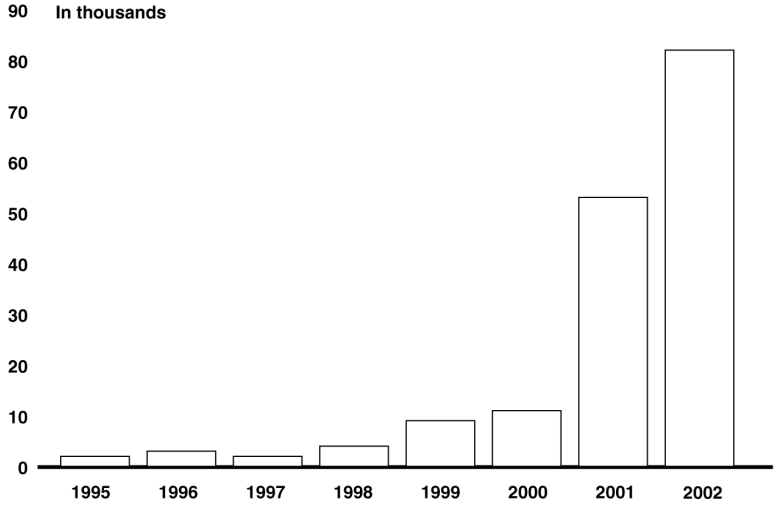
Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center[6] has also risen dramatically from 9,859 in 1999 to 52,658 in 2001 and 82,094 in 2002. And these are only the reported attacks. The Director of CERT Centers stated

[5]*Virus:* a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse:* a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm:* an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb:* in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer:* synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

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

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 (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. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, 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 terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was

discovered on computers found in al Qaeda camps in Afghanistan.[7] Also, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[8] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Since September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized. In his November 2002 congressional testimony, 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.[9] 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.

The risks posed by this increasing and evolving threat are demonstrated in reports of actual and potential attacks and disruptions. For example:

[7]"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).

[8]Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.

[9]Testimony 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.

- On February 11, 2003, the National Infrastructure Protection Center (NIPC) issued an advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq.[10] This advisory noted that during a time of increased international tension, illegal cyber activity often escalates, such as spamming, Web page defacements, and denial-of-service attacks. Further, this activity can originate within another country that is party to the tension; can be state sponsored or encouraged; or can come from domestic organizations or individuals independently. The advisory also stated that attacks may have one of several objectives, including political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers, political activism or disruptive attacks targeting United States systems by those opposed to any potential conflict with Iraq, or even criminal activity masquerading or using the current crisis to further personal goals.

- According to a preliminary study coordinated by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest computer worm in history. As the study reports, exploiting a known vulnerability for which a patch has been available since July 2002, Slammer doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages and such unforeseen consequences as canceled airline flights and automated teller machine (ATM) failures. Further, the study emphasizes that the effects would likely have been more severe had Slammer carried a malicious payload, attacked a more widespread vulnerability, or targeted a more popular service.

- In November 2002, news reports indicated that a British computer administrator was indicted on charges that he broke into 92 U.S. computer networks in 14 states; these networks belonged to the Pentagon, private companies, and the National Aeronautics and Space Administration during the past year, causing some $900,000 in damage to computers. According to a Justice Department official, these attacks were one of the biggest hacks ever against the U.S. military. This official also said that the attacker used his home computer and automated software available on the Internet

[10]National Infrastructure Protection Center, *National Infrastructure Protection Center Encourages Heightened Cyber Security as Iraq—U.S. Tensions Increase*, Advisory 03-002 (Washington, D.C.: Feb. 11, 2003).

to scan tens of thousands of computers on U.S. military networks looking for ones that might suffer from flaws in Microsoft Corporation's Windows NT operating system software.

- On October 21, 2002, NIPC reported that all the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive "distributed denial of service" attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages.

- In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[11] 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. In addition, a swarming attack could 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. Consistent with this threat, NIPC also released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[12]

- In August 2001, we reported to a subcommittee of the House Government Reform Committee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. Then in September 2001, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus that allowed it to spread widely in a short amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage.[13]

[11]National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

[12]National Infrastructure Protection Center, *Possible Terrorism Targeting of US Financial System*–Information Bulletin 02-003 (Washington, D.C.: Apr. 19, 2002).

[13]U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures;* GAO-01-1073T (Washington, D.C.: Aug. 29, 2001).

Significant Weaknesses Persist in Federal Information Security

For the federal government, we have reported since 1996 that poor information security is a widespread 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 2003.[16]

As we reported in November 2002, our analyses of reports issued from October 2001 through October 2002, continued 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,[18] 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

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

[15]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious* and *Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001), and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-02-303T (Washington, D.C.: Nov. 19, 2002).

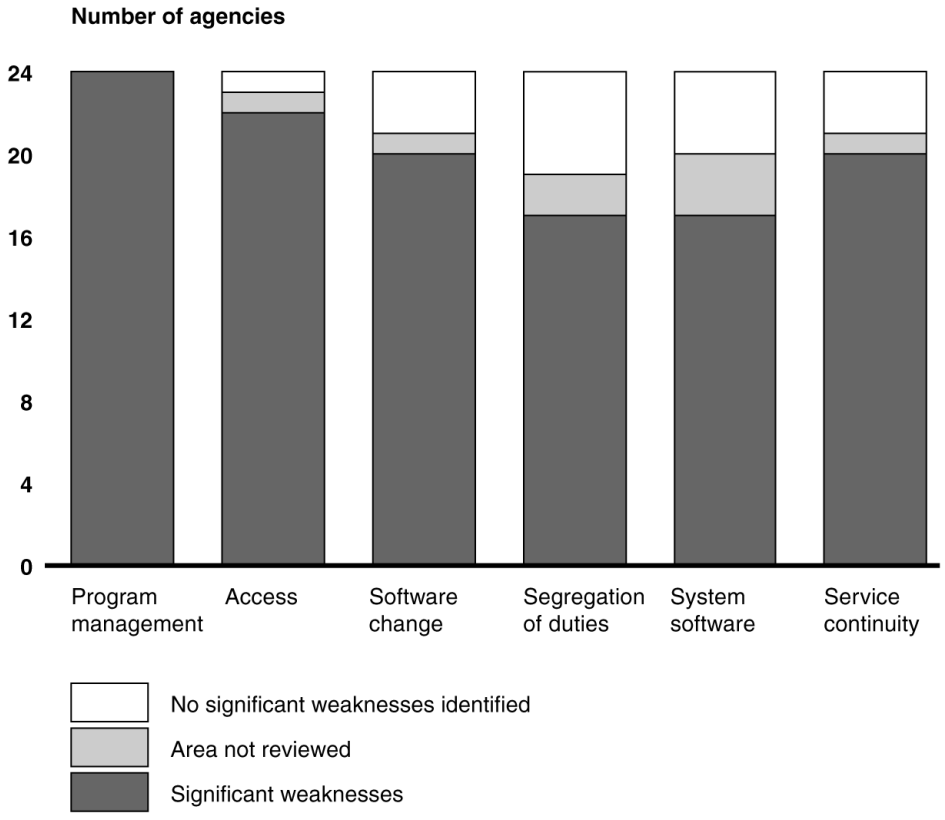
[16]GAO-03-121.

[17]GAO-03-303T.

[18]Does not include the Department of Homeland Security that was created by the Homeland Security Act in November 2002.

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 2 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 2: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued October 2001 through October 2002.

Although our analyses showed that most agencies had significant weaknesses in these six control areas, as in past years' analyses, weaknesses were most often identified for security program management and access controls.

- *For security program management*, we identified weaknesses for all 24 agencies in 2002—the same as reported for 2001, and compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

- *For access controls*, we found weaknesses for 22 of 24 agencies (92 percent) in 2002 (no significant weaknesses were found for one agency, and access controls were not reviewed for another). This compares to access control weaknesses found in all 24 agencies for both 2000 and 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

  Our analyses also showed service-continuity-related weaknesses at 20 of the 24 agencies (83 percent) with no significant weaknesses found for 3 agencies (service continuity controls were not reviewed for another). This compares to 19 agencies with service continuity weaknesses found in 2001 and 20 agencies found in 2000. Service continuity controls are important in that they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission. Further, such controls are particularly important in the wake of the terrorist attacks of September 11, 2001.

  These analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step

toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 2 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as DOD and the Department of Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. However, in response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems has also increased as agencies and their IGs reviewed and evaluated their information security programs as required by GISRA.

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

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.

Congress Consolidates and Strengthens Federal Information Security Requirements

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, Congress enacted GISRA, which became effective November 29, 2000, for a period of 2 years. GISRA supplemented information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and was consistent with existing information security guidance issued by the Office of Management and Budget (OMB)[19] and the National Institute of Standards and Technology (NIST),[20] as well as audit and best practice guidance issued by GAO.[21]

Most importantly, however, GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. GISRA assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and IGs. OMB was responsible for establishing and overseeing policies, standards, and guidelines for

[19]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

[20]Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.

[21]U.S. General Accounting Office, *Federal Information System Controls Manual*, *Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

information security. This included the authority to approve agency information security programs, but delegated OMB's responsibilities regarding national security systems to national security agencies. OMB was also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. GISRA does not specify a date for this report, and OMB released its fiscal year 2001 report in February 2002. It has not yet released its fiscal year 2002 report.

GISRA required each agency, including national security agencies, to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program was to include

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;
- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- an annual program review by agency program officials.

In addition to the responsibilities listed above, GISRA required each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non-national-security systems were to be performed by the agency IG or an independent evaluator, and the results of these evaluations were to be reported to OMB. For the evaluation of national security systems, special provisions included having national

security agencies designate evaluators, restricting the reporting of evaluation results, and having the IG or an independent evaluator perform an audit of the independent evaluation. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

With GISRA expiring on November 29, 2002, on December 17, 2002, FISMA was enacted as title III of the E-Government Act of 2002. This act permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA. In addition, among other things, FISMA requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. In addition, FISMA requires each agency to develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is also to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

Agencies Show Progress in Implementing Security Requirements, but Further Improvement Needed

In our March 2002 testimony, we reported that the initial implementation of GISRA was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses.[22] Agencies also noted benefits of this first-year implementation, including increased management attention to and accountability for information security, and the administration undertook other important actions to address information security, such as integrating information security into the President's Management Agenda Scorecard. However, along with these benefits, agencies' reviews of their information security programs showed that agencies had not established information security programs consistent with the legislative requirements and that significant weaknesses existed. We also noted that although agency actions were under way to strengthen information security and

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

implement these requirements, significant improvement would require sustained management attention and OMB and congressional oversight.

Our analysis of second-year or fiscal year 2002 implementation of GISRA showed progress in several areas, including the types of information being reported and made available for oversight, governmentwide efforts to improve information security, and agencies' implementation of information security requirements. Despite this progress, our analyses of agency and IG reports showed that the 24 agencies have not yet established information security programs consistent with legislative requirements and that corrective action plans did not always include all identified weaknesses and need independent validation to ensure that weaknesses are corrected.

OMB Includes New Reporting Requirements to Improve Information Available for Oversight

For fiscal year 2002 GISRA reporting, OMB provided the agencies with updated reporting instructions and guidance on preparing and submitting plans of action and milestones (corrective action plans).[23] Like instructions for fiscal year 2001, this updated guidance listed specific topics that the agencies were to address, many of which were referenced back to corresponding requirements of GISRA.[24] However, in response to agency requests and recommendations we made to OMB as a result of our review of fiscal year 2001 GISRA implementation,[25] this guidance also incorporated several significant changes to help improve the consistency and quality of information being reported for oversight by OMB and the Congress. These changes included the following:

- Reporting instructions provided new high-level management performance measures that the agencies and IGs were required to use to report on agency officials' performance. According to OMB, most agencies did not

[23]"Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," Memorandum for Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., M-02-09, July 2, 2002.

[24]OMB required the agency heads to submit their reports on September 16, 2002, and to include (1) the executive summary developed by the agency CIO, agency program officials, and the IG that is based on the results of their work; (2) copies of the IG's independent evaluations; and (3) for national security systems, audits of the independent evaluations. Agencies' corrective action plans were due to OMB by October 1, 2002, with updates required quarterly beginning January 1, 2003.

[25]U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-407 (Washington, D.C.: May 2, 2002).

provide performance measures or actual levels of performance where asked to do so for fiscal year 2001 reporting, and the agencies requested that OMB develop such measures. These required performance measures include, for example, the number and percentage of systems that have been assessed for risk, the number of contractor operations or facilities that were reviewed, and the number of employees with significant security responsibilities that received specialized training.

- Instructions confirmed that agencies were expected to review all systems annually. OMB explained that GISRA requires senior agency program officials to review each security program for effectiveness at least annually, and that the purpose of the security programs discussed in GISRA is to ensure the protection of the systems and data covered by the program. Thus, a review of each system is essential to determine the program's effectiveness, and only the depth and breadth of such system reviews are flexible.

- Agencies were generally required to use all elements of NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, to review their systems. This guide accompanies NIST's Security Assessment Framework methodology, which agency officials can use to determine the current status of their security programs.[26] The guide itself uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. For the fiscal year 2001 reporting period, OMB encouraged agencies to use this guide, but did not require its use because it was not completed until well into the reporting period. NIST finalized the guide in November 2001, and for fiscal year 2002 reporting, OMB required its use unless an agency and its IG confirmed that any agency-developed methodology captured all elements of the guide. To automate the completion of the questionnaire, NIST also developed a tool that can be found at its Computer Security Resource Center Web site: http://csrc.nist.gov/asset/.

- OMB requested IGs to verify that agency corrective action plans identify all known security weaknesses within an agency, including components, and are used by the IG and the agency, major components, and program officials within them, as the authoritative agency management mechanism

[26]National Institute of Standards and Technology, *Federal Information Technology Security Assessment Framework*, prepared for the Federal CIO Council by the NIST Computer Security Division Systems and Network Security Group, Nov. 28, 2000.

to prioritize, track, and manage all agency efforts to close security performance gaps.

- OMB authorized agencies to release certain information from their corrective action plans to assist the Congress in its oversight responsibilities. Agencies could release this information, as requested, excluding certain elements, such as estimated funding resources and the scheduled completion dates for resolving a weakness.

OMB Initiatives to Improve Federal Information Security Show Progress

OMB's report to the Congress on fiscal year 2001 GISRA implementation provided an overview of OMB and agencies' implementation efforts, summarized the overall results of OMB's analyses, and included individual agency summaries for the 24 of the largest federal departments and agencies.[27] Overall, OMB reported that although examples of good security exist in many agencies, and others were working very hard to improve their performance, many agencies had significant deficiencies in every important area of security. In particular, the report highlighted six common security weaknesses. These weaknesses are listed below along with an update of the activities under way to address them.

1. *Lack of senior management attention to information security*—Last year, OMB reported that, to address this issue, it was working through the President's Management Council and the Critical Infrastructure Protection Board to promote sustained attention to security as part of its work on the President's Management Agenda and the integration of security into the Scorecard. OMB also reported that it included security instructions in budget passback guidance and sent security letters to each agency highlighting the lack of senior management attention and describing specific actions OMB is taking to assist the agency. According to OMB officials, although the President's Critical Infrastructure Protection Board was recently dissolved, OMB continues to coordinate security issues with the President's Homeland Security Council and the Department of Homeland Security. These officials also said that they are continuing to work with the agencies and that security is an integral part of assessing agencies' performance for the E-Government component of the Scorecard.

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

2. *Inadequate accountability for job and program performance related to IT security*—OMB reported that it was working with the agencies and other entities to develop workable measures of job and program performance to hold federal employees accountable for their security responsibilities. As discussed previously, OMB instructions to federal agencies for fiscal year 2002 GISRA reporting included high-level management performance measures. Related to this initiative, in October 2002, NIST also issued an initial public draft of a security metrics guide for IT systems to provide guidance on how an organization, through the use of metrics, can determine the adequacy of in-place security controls, policies, and procedures. The draft also explains the metric development and implementation process and how it can also be used to adequately justify security control investments.[28]

3. *Limited security training for general users, IT professionals, and security professionals*—OMB reported that along with federal agencies, it was working through the Critical Infrastructure Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. OMB also reported that work was under way to identify and disseminate security training best practices through NIST's Federal Agency Security Practices Web site and that one of the administration's electronic government initiatives is to establish and deliver electronic-training on a number of mandatory topics, including security, for use by all federal agencies, along with state and local governments. As an example of progress on this initiative, OMB officials pointed to an online training initiative, www.golearn.gov. Launched in July 2002 by the Office of Personnel Management (OPM), this site offers training in an online environment, including IT security courses, such as security awareness, fundamentals of Internet security, and managing network security. Other activities for this area include NIST's July 2002 issuance of draft guidance on designing, developing, implementing, and maintaining an awareness and training program within an agency's IT security program.[29]

4. *Inadequate integration of security into the capital planning and investment control process*—OMB reported that it was integrating

[28]National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems,* NIST Draft Special Publication 800-55 (October 2002).

[29]National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, NIST Draft Special Publication 800-50 (July 19, 2002).

security into the capital planning and investment control process to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Specifically, OMB established criteria that agencies must report security costs for each major and significant IT investment, document in their business cases that adequate security controls have been incorporated into the life cycle planning and funding of each IT investment, and tie their corrective action plans for a system directly to the business case for that IT investment. Another criterion was that agency security reports and corrective action plans were presumed to reflect the agency's security priorities and, thus, would be a central tool for OMB in prioritizing funding for systems. OMB officials confirmed that these activities were continuing and included providing additional guidance in OMB Circular A-11 on identifying security costs. In addition, they said that draft NIST guidelines for federal IT systems would help to ensure that agencies consider security throughout the system life cycle.[30] Under OMB policy, responsible federal officials are required to make a security determination (called accreditation) to authorize placing IT systems into operation. In order for these officials to make sound, risk-based decisions, a security evaluation (known as certification) of the IT system is needed. The NIST guidelines are to establish a standard process, general tasks and specific subtasks to certify and accredit systems and provide a new approach that uses the standardized process to verify the correctness and effectiveness of security controls employed in a system. The guidelines will also employ the use of standardized, minimum security controls and standardized verification techniques and procedures that NIST indicates will be provided in future guidance.

5. *Poor security for contractor-provided services*—OMB reported last year that under the guidance of the OMB-led security committee established by Executive Order 13231 (since eliminated), an issue group would develop recommendations to include addressing how security is handled in contracts. OMB also reported that it would work with the CIO Council and the Procurement Executives Council to establish a training program that ensures appropriate contractor training in security. OMB officials stated that these activities are continuing and the issue group had made recommendations to the Federal Acquisition Regulation Council. In addition, in October 2002,

[30]National Institute of Standards and Technology, *Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems*, NIST Draft Special Publication 800-37 (Oct. 28, 2002).

NIST issued a draft guide on security considerations in federal IT procurements, which includes specifications, clauses, and tasks for areas such as IT security training and awareness, personnel security, physical security, and security features in systems.[31]

6. *Limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections*—OMB reported that the Federal Computer Incident Response Center (FedCIRC) reports to it on a quarterly basis on the federal government's status on IT security incidents. OMB also reported that under OMB and Critical Infrastructure Protection Board guidance, GSA was exploring methods to disseminate patches to all agencies more effectively. OMB officials pointed to the Patch Authentication and Dissemination Capability Program, which FedCIRC introduced in January 2003 as a free service to federal civilian agencies.[32] According to FedCIRC, this service provides a trusted source of validated patches and notifications on new threats and vulnerabilities that have potential to disrupt federal government mission critical systems and networks. It is a Web-enabled service that obtains patches from vendors, validates that the patch only does what it states that it was created to correct, and provides agencies notifications based on established profiles. We also noted that in August 2002, NIST published procedures for handling security patches that provided principles and methodologies for establishing an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.[33]

In addition to activities identified for these specific weaknesses, in last year's report, OMB reported that it would direct all large agencies to undertake a Project Matrix review to more clearly identify and prioritize the security needs for government assets. Project Matrix is a methodology

[31]National Institute of Standards and Technology, *Security Considerations in Federal Information Technology Procurements: A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials*, NIST Draft Special Publication 800-4A (Oct. 9, 2002).

[32]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide 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.

[33]National Institute of Standards and Technology, *Procedures for Handling Security Patches—Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-40 (August 2002).

developed by the Critical Infrastructure Assurance Office (CIAO) (recently transferred to the Department of Homeland Security) that identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector.[34] OMB reported that once reviews have been completed at each large agency, it would identify cross-government activities and lines of business for Project Matrix reviews so that it will have identified both vertically and horizontally the critical operations and assets of the federal government's critical enterprise architecture and their relationship beyond government.

As of July 2002, a CIAO official reported that of 31 agencies targeted for Project Matrix reviews, 18 had begun their reviews; and of those, 5 had completed the first step of the methodology to identify their critical assets, 2 found no candidate assets to undergo a process to identify critical assets, 5 had begun the second step to identify other federal government assets, systems, and networks upon which their critical assets depend to operate, and none had begun the third step to identify all associated dependencies on private-sector owned and operated critical infrastructures.[35] According to a CIAO official in December 2003, the office's goal was 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 official also said that at the request of the Office of Homeland Security, CIAO was revising and streamlining its Project Matrix methodology to be less labor intensive for the agencies and reduce the time needed to identify critical assets. In our recent discussions with OMB officials, they said they were requiring Project Matrix reviews for 24 large departments and agencies and that as part of their GISRA reporting, agencies were required to report on the status of their efforts to identify critical assets and their dependencies. However, they acknowledged that OMB did not establish any deadlines for the completion of Project Matrix reviews. In our February 2003 report, we also reported that neither the administration nor

[34]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, 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.

[35]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

the agencies we reviewed had milestones for the completion of Project Matrix analyses and recommended that agencies coordinate with CIAO to set these milestones.

Finally, in February 2002, OMB reported that a number of efforts were under way to address security weaknesses in industry software development, and that chief among them were national policy-level activities of the Critical Infrastructure Protection Board (since eliminated). At the technical product-level, OMB reported that the National Information Assurance Partnership, operated jointly by NIST and the National Security Agency, was certifying private-sector laboratories to which product vendors may submit their software for analysis and certification, but that this certification process was a lengthy one and often cannot accommodate the "time-to-market" imperative that the technology industry faces. According to recent discussions with OMB officials, the National Information Assurance Partnership efforts are still under way.

Agency GISRA Reporting Shows Progress, but Highlights Continued Weaknesses

Fiscal year 2002 GISRA reporting by CIOs and independent evaluations by IGs for the 24 agencies provided an improved baseline for measuring improvements in federal information security not only because of performance measures that OMB now requires, but also because of agencies' increased review coverage and use of consistent methodologies. For example, 16 agencies reported that they had reviewed the security of 60 percent or more of their systems and programs for their fiscal year 2002 GISRA reporting, with 10 of these reporting that they reviewed from 90 to 100 percent. Further, 13 agencies reported that coverage of agency systems and programs increased for fiscal year 2002 compared to fiscal year 2001. However, with 8 agencies reporting that they reviewed less than half of their systems, improvements are still needed.[36] Regarding their methodologies, 21 agencies reported that, as required by OMB, they used NIST's *Security Self-Assessment Guide for Information Technology Systems* or developed their own methodology that addressed all elements of the guide, and only 3 agencies reported that they did not. By not following the NIST guide, agencies may not identify all weaknesses. For example, one agency reported that the methodology it used incorporated many of the elements of NIST's self-assessment guide, but the IG reported

[36]One agency did not specifically report this information, but its IG reported that the agency reviewed less than half of its systems.

that the methodology did not call for the detailed level of system reviews required by the NIST guide nor did it include the requirement to test and evaluate security controls.

In performing our analyses, we summarized and categorized the reported information including data provided for the OMB-prescribed performance measures. There were several instances where agency reports either did not address or provide sufficient data for a question or measure. In addition, IGs' independent evaluations sometimes showed different results than CIO reporting or identified data inaccuracies. Further, IG reporting also did not always include comparable data, particularly for the performance measures. In part, this was because although OMB instructions said that the IGs should use the performance measures to assist in evaluating agency officials' performance, the IG was not required to review the agency's reported measures. Summaries of our analyses for key requirements follow below.

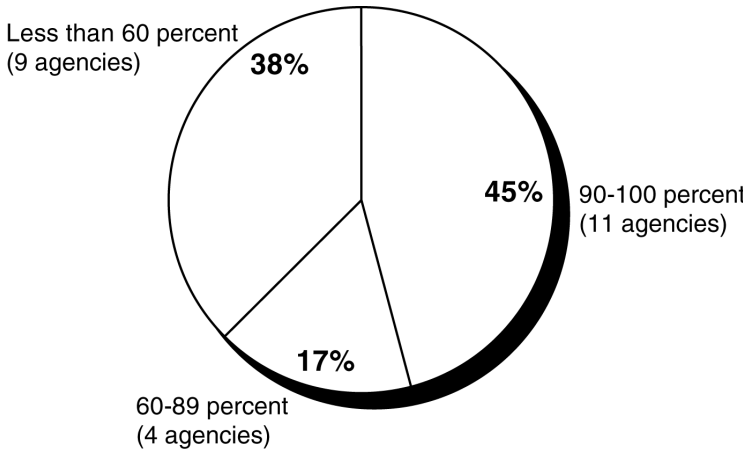
Many Systems Still Do Not Have Risk Assessments or Up-to-Date Security Plans

GISRA required agencies to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk management and overall security program management and, as our best practice work has shown, are an integral part of the management processes of leading organizations.[37] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Our reviews of federal agencies, however, frequently show deficiencies related to assessing risk, such as security plans for major systems that are not developed on the basis of risks. As a result, the agencies had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable.

[37] GAO/AIMD-98-68.

As one of its performance measures for this requirement, OMB required agencies to report the number and percentage of their systems that have been assessed for risk during fiscal year 2001 and fiscal year 2002. Our analyses of reporting for this measure showed some overall progress. For example, of the 24 agencies we reviewed, 13 reported an increase in the percentage of systems assessed for fiscal year 2002 compared to fiscal year 2001. In addition, as illustrated in figure 3 below, for fiscal year 2002, 11 agencies reported that they had assessed risk for 90 to 100 percent of their systems. However, it also shows that further efforts are needed by other agencies, including the 9 that reported less than 60 percent of their systems had been assessed for risk.

Figure 3: Percentage of systems with risk assessments during fiscal year 2002



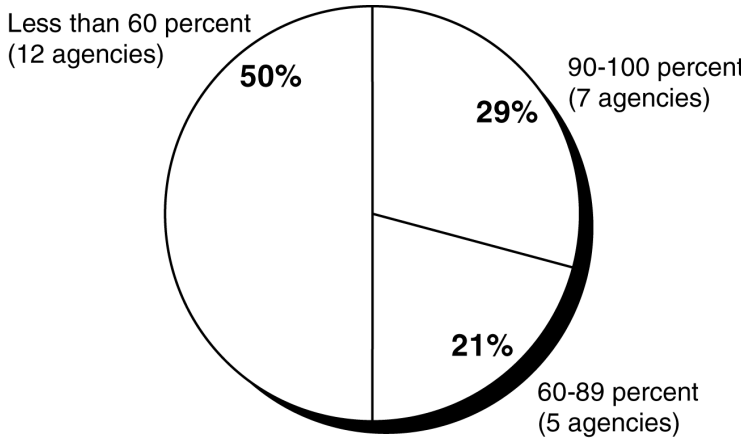
Source: Agency-reported data.

Note: Rounding used to total 100 percent.

GISRA also required the agency head to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. In its reporting instructions, OMB required agencies to report whether the agency head had taken specific and direct actions to oversee that program officials and the CIO are ensuring that security plans are up to date and practiced throughout the life cycle. They also had to report the number and percentage of systems that have an up-to-date security plan. Our analyses showed that although most agencies reported that they had taken such actions, IG reports disagreed for a number of agencies, and many systems do not have up-to-date security plans. Specifically, 21 agencies reported that the agency head had taken actions to oversee that security plans are up to date and practiced throughout the life cycle compared to the IGs reporting that only 9 agencies had taken

such actions. One IG reported that the agency's security plan guidance predates revisions to NIST and OMB guidance and, as a result, does not contain key elements, such as the risk assessment methodology used to identify threats and vulnerabilities. In addition, another IG reported that although progress had been made, security plans had not been completed for 62 percent of the agency's systems. Regarding the status of agencies' security plans, as shown in figure 4, half of the 24 agencies reported that they had up-to-date security plans for 60 percent or more of their systems for fiscal year 2002, including 7 that reported these plans for 90 percent or more.

Figure 4: Percentage of systems with up-to-date security plans during fiscal year 2002



Source: Agency-reported data.

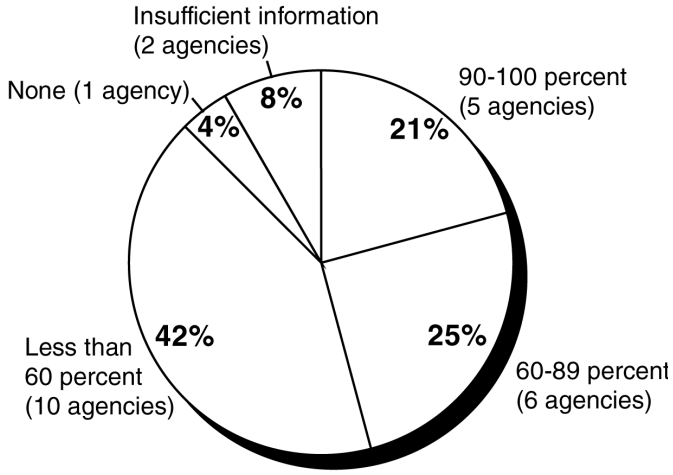
Security Training Efforts Show Mixed Progress

GISRA required agencies to provide training on security awareness for agency personnel and on security responsibilities for information security personnel. Our studies of best practices at leading organizations have shown that they took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. However, our past information security reviews at individual agencies have shown that they have not provided adequate computer security training to their employees, including contractor staff.

Among the performance measures for these requirements, OMB required agencies to report the number and percentage of employees including contractors that received security training during fiscal years 2001 and 2002 and the number of employees with significant security responsibilities that received specialized training. For agency employee/contractor security training, our analyses showed 16 agencies reported that they provided security training to 60 percent or more of their employees and contractors for fiscal year 2002, with 9 reporting 90 percent or more. Of the remaining 8 agencies, 4 reported that such training was provided for less than half of their employees/contractors, 1 reported that none were provided this training, and 3 provided insufficient data for this measure.

For specialized training for employees with significant security responsibilities, some progress was indicated, but additional training is needed. As indicated in figure 5, our analyses showed 11 agencies reported that 60 percent or more of their employees with significant security responsibilities had received specialized training for fiscal year 2002, with 5 reporting 90 percent or more. Of the remaining 13 agencies, 4 reported less than 30 percent and one reported that none had received such training.

Figure 5: Percentage of employees with significant security responsibilities receiving specialized security training during fiscal year 2002



Source: Agency-reported data.

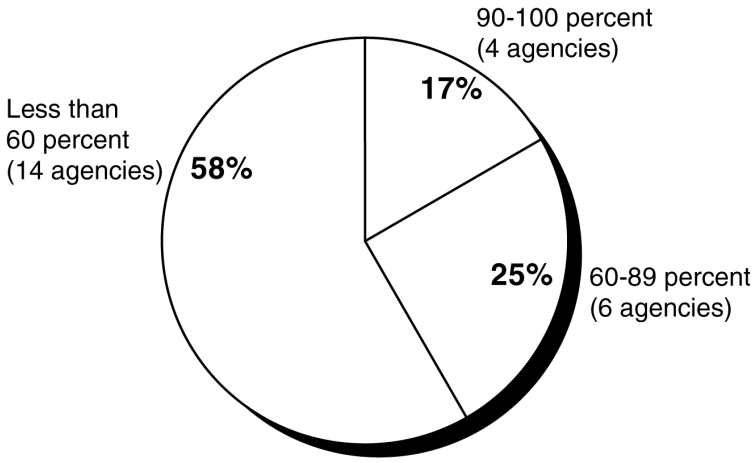
Further Security Control Testing and Evaluation Needed

Under GISRA, the agency head was responsible for ensuring that the appropriate agency officials, evaluated the effectiveness of the information security program, including testing controls. The act also required that the agencywide information security program include periodic management testing and evaluation of the effectiveness of information security policies and procedures. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of the program reviews can supplement control testing and evaluation in IG and GAO audits to help provide a more complete picture of the agencies' security postures.

As a performance measure for this requirement, OMB required the agencies to report the number and percentage of systems for which security controls have been tested and evaluated during fiscal years 2001 and 2002. Our analyses of the data agencies reported for this measure showed that although 15 agencies reported an increase in the overall percentage of systems being tested and evaluated for fiscal year 2002, most agencies are not testing essentially all of their systems. As shown in figure 6, our analyses showed that 14 agencies reported that they had

tested the controls of less than 60 percent of their systems for fiscal year 2002. Of the remaining 10 agencies, 4 reported that they had tested and evaluated controls for 90 percent or more of their systems.

Figure 6: Percentage of systems with security controls tested during fiscal year 2002

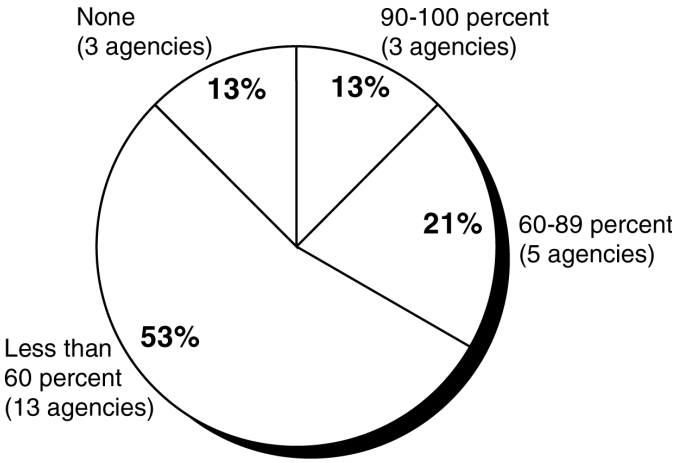


Source: Agency-reported data.

As another measure, OMB also required agencies to report the number and percentage of systems that have been authorized for processing following certification and accreditation. According to NIST's draft *Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems* (Special Publication 800-37), accreditation is the authorization of an IT system to process, store, or transmit information, granted by a management official that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. *Certification* is the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. The accreditation decision is based on the implementation of an agreed upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it.

Our analysis of agencies' reports showed mixed progress for this measure. For example, 10 agencies reported increases in the percentage of systems authorized for processing following certification and accreditation compared to fiscal year 2001, but 8 reported decreases and 3 did not change (3 others did not provide sufficient data). In addition, as shown in figure 7, 8 agencies reported that for fiscal year 2002, 60 percent or more of their systems had been authorized for processing following certification and accreditation with only 3 of these reporting from 90 to 100 percent. And of the remaining 16 agencies reporting less than 60 percent, 3 reported that none of their systems had been authorized.

Figure 7: Percentage of systems during fiscal year 2002 that are authorized for processing by management after certification and accreditation



Source: Agency-reported data.

In addition to this mixed progress, IG reports identified instances where agencies' certification and accreditation efforts were inadequate. For example, one agency reported that 43 percent of its systems were authorized for processing following certification and accreditation. IG reporting agreed, but also noted that over a fourth of the systems identified as authorized had been operating with an interim authorization and did not meet all of the security requirements to be granted accreditation. The IG also stated that, due to the risk posed by systems operating without certification and full accreditation, the department should consider identifying this deficiency as a material weakness.

Incident-Handling Capabilities Established, but Implementation Incomplete

GISRA required agencies to implement procedures for detecting, reporting, and responding to security incidents. Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management. Our information security reviews also confirm that federal agencies have not adequately (1) prevented intrusions before they occur, (2) detected intrusions as they occur, (3) responded to successful intrusions, or (4) reported intrusions to staff and management. Such weaknesses provide little assurance that unauthorized attempts to access sensitive information will be identified and appropriate actions taken in time to prevent or minimize damage.

OMB included a number of performance measures in agency reporting instructions that were related to detecting, reporting, and responding to security incidents. These included the number of agency components with an incident-handling and response capability, whether the agency and its major components share incident information with FedCIRC in a timely manner, and the numbers of incidents reported. OMB also required that agencies report on how they confirmed that patches have been tested and installed in a timely manner. Our analyses of agencies' reports showed that although most agencies reported that they have established incident response capabilities, implementation of these capabilities is still not complete. For example, 12 agencies reported that for fiscal year 2002, 90 percent or more of their components had incident handling and response capabilities and 8 others reported that they provided these capabilities to components through a central point within the agency. However, although most agencies report having these capabilities for most components, in at least two instances, the IGs' evaluations identified instances where incident response capabilities were not always implemented. For example, one IG reported that the department established and implemented its computer security incident-response capability on August 1, 2002, but had not enforced procedures to ensure that components comply with a consistent methodology to identify, document, and report computer security incidents. Another IG reported that the agency had released incident-handling procedures and established a computer incident

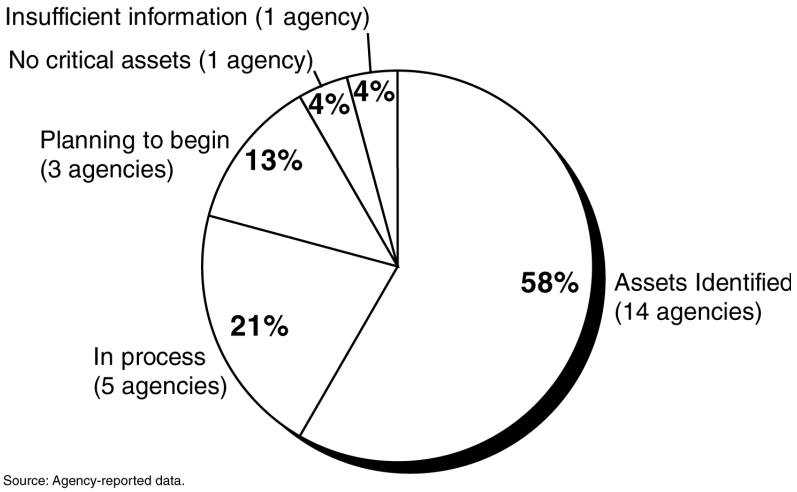
response team, but had not formally assigned members to the team or effectively communicated procedures to employees.

Our analyses also showed that for fiscal year 2002, 13 agencies reported they had oversight procedures to verify that patches have been tested and installed in a timely manner and 10 reported they did not. Of those that did not have procedures, several specifically mentioned that they planned to participate in FedCIRC's patch management process.

Agencies Show Progress in Identifying Critical Assets, but Most Have Not Identified Interdependencies

GISRA required that each agencywide information security program ensure the integrity, confidentiality, and availability of systems and data supporting the agency's critical operations and assets. In addition, as mentioned previously, OMB directed 24 of the largest agencies to undergo a Project Matrix review to identify and characterize the operations and assets and these assets' associated infrastructure dependencies and interdependencies that are most critical to the nation. For example, as part of its GISRA reporting, OMB required the agencies to report whether they had undergone a Project Matrix review or used another methodology to identify their critical assets and their interdependencies and interrelationships. Our analyses of agencies' reports showed some overall process in identifying critical assets, but limited progress in identifying interdependencies. As shown in figure 8, a total of 14 agencies reported they had identified their critical assets and operations—10 using Project Matrix and 4 using other methodologies. In addition, five more agencies reported that they were in some stage of identifying their critical assets and operations, and three more planned to do so in fiscal year 2003.

Figure 8: Percentage of agencies that had identified their critical assets and operations—fiscal year 2002



Source: Agency-reported data.

Our analyses also showed that three agencies reported they had identified the interdependencies for their critical assets, and four others reported that they were in some stage of undertaking this process.

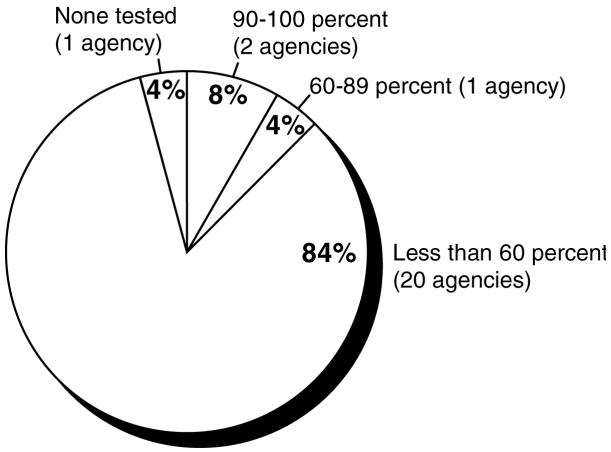
Lack of Contingency Plan Testing Is a Major Weakness

Contingency plans provide specific instructions for restoring critical systems, including such things as arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. At many of the agencies we have reviewed, we found incomplete plans and procedures to ensure that critical operations can continue when unexpected events occur, such as a temporary power failure, accidental loss of files, or a major disaster. These plans and procedures were incomplete because operations and supporting resources had not been fully analyzed to determine which were most critical and would need to be restored first. Further, existing plans were not fully tested to identify their weaknesses. As a result, many agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

As another of its performance measures, OMB required agencies to report the number and percentage of systems for which contingency plans have been tested in the past year. As shown in figure 9, our analyses showed that for fiscal year 2002, only 2 agencies reported they had tested contingency plans for 90 percent or more of their systems, while 20 had

tested contingency plans for less than 60 percent of their systems. One reported that none had been tested.

Figure 9: Percentage of systems with recently tested contingency plans for fiscal year 2002



Source: Agency-reported data.

Note: Rounding used to total 100 percent.

Some Reported Improvement in Efforts to Ensure Security of Contractor-Provided Services

GISRA requires agencies to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained either by the agency or for it by another agency or contractor. In its fiscal year 2001 GISRA report to the Congress, OMB identified poor security for contractor-provided services as a common weakness and for fiscal year 2002 reporting, included performance measures to help indicate whether the agency program officials and CIO used appropriate methods, such as audits and inspections, to ensure that service provided by a contractor are adequately secure and meet security requirements. Our analyses showed that a number of agencies reported that they have reviewed a large percentage of services provided by a contractor, but others have reviewed only a small number.

For operations and assets under the control of agency program officials, 16 agencies reported that for fiscal year 2002 they reviewed 60 percent or more of contractor operations or facilities, with 7 of these reporting that they reviewed 90 percent or more; and 4 reported that they reviewed less than 30 percent.

For operations and assets under the control of the CIO, 11 agencies reported that for fiscal year 2002 they reviewed 60 percent or more of contractor operations or facilities, with 7 of these reporting they reviewed 90 percent or more; 3 reported that they reviewed less than 30 percent; and 5 agencies reported that they had no services provided by a contractor or another agency.

Reporting of Security Costs Shows Improvement

GISRA requires that each agency examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports related to annual agency budgets and other statutory performance reporting requirements. The act also requires each agency to describe the resources, including budget, staffing, and training, that are necessary to implement its agencywide information security program. For GISRA reporting, OMB required agencies to report information on total security funding included in their fiscal year 2002 budget request, fiscal year 2002 budget enacted, and the President's fiscal year 2003 budget and to include (1) a breakdown of security costs by each major operating division or bureau and (2) CIP costs that apply to the protection of government operations and assets.

Most agencies (21) reported total security funding for these budgets, although 13 did not show costs by major operating division or bureau and/or for CIP. Further, most agencies reported including security costs in their budget requests and justifications. For example:

- For the fiscal year 2003 budget, 16 agencies reported that they had submitted capital asset plans and justifications to OMB with all requisite security information, and of the remaining 8 agencies, 5 reported that less than 30 percent of their capital asset plans and justifications did not include this information. Last year, 19 agencies reported that they had not included security requirements and costs on every fiscal year 2002 capital asset plan submitted to OMB.

- For fiscal year 2003, 18 agencies reported that security costs were reported on the Exhibit 53[38] for all agency systems, with 5 reporting that these costs were not reported for all agency systems.

[38]The Agency IT Investments Portfolios as required by OMB Circular A-11.

Corrective Action Plans Provide Potential Tool for Monitoring Agency Progress

GISRA required that agencies develop a process for ensuring that remedial action is taken to address significant deficiencies. As a result, OMB required the agency head to work with the CIO and program officials to provide a strategy to correct security weaknesses identified through annual GISRA program reviews and independent evaluations, as well as other reviews or audits performed throughout the reporting period by the IG or GAO. Agencies were required to submit a corrective action plan for all programs and systems where a security weakness had been identified plus quarterly updates on the plan's implementation. OMB guidance required that these plans list the identified weaknesses and for each identify a point of contact, the resources required to resolve the weakness, the scheduled completion date, key milestones with completion dates for the milestones, milestone changes, the source of the weakness (such as a program review, IG audit, or GAO audit), and the status (ongoing or completed). Agencies were also required to submit quarterly updates of these plans that list the total number of weaknesses identified at the program and system level, as well as the numbers of weaknesses for which corrective actions were completed on time, ongoing and on schedule, or delayed. Updates were also to include the number of new weaknesses discovered subsequent to the last corrective action plan or quarterly update.

Our analyses of agencies' fiscal year 2002 corrective action plans and IGs' evaluations of these plans showed that most agencies followed the OMB-prescribed format, but also that several used an existing tracking system to meet this requirement. In theory, these plans could prove to be a useful tool for the agencies in correcting their information security weaknesses. However, their usefulness could be impaired to the extent that they do not identify all weaknesses or provide realistic completion estimates. For example, for the 24 agencies, only 5 IGs reported that their agency's corrective action plan addressed all identified significant weaknesses and 9 specifically reported that their agency's plan did not. Our analyses also showed that in several instances, corrective action plans did not indicate the current status of weaknesses identified or include information regarding whether actions were on track as originally scheduled.

Plan progress must be appropriately monitored and the actual correction of weaknesses may require independent validation. Our analyses showed that three IGs reported that their agencies did not have a centralized tracking system to monitor the status of corrective actions. Also, one IG specifically questioned the accuracy of unverified, self-reported corrective actions reported in the agency's plan.

Further Action Needed to Improve Federal Information Security

Recent audits and reviews, including annual GISRA program reviews and independent evaluations, show that although agencies have made progress in addressing GAO and IG recommendations to improve the effectiveness of their information security, further action is needed. In particular, overall security program management continues to be an area marked by widespread and fundamental problems. Many agencies have not developed security plans for major systems based on risk, have not documented security policies, and have not implemented a program for testing and evaluating the effectiveness of the controls they rely on. As a result, they could not ensure that the controls they had implemented were operating as intended and they could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Further information security improvement efforts are also needed at the governmentwide level, and it is important that these efforts are guided by a comprehensive strategy and, as development of this strategy continues, that certain key issues be addressed. These issues and actions currently under way are as follows.

First, the federal strategy should delineate the roles and responsibilities of the numerous entities involved in federal information security and describe how the activities of these organizations interrelate, who should be held accountable for their success or failure, and whether these activities will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding which computer security controls to implement and the level of rigor with which to enforce these controls. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[39] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. FISMA requires NIST to develop standards that provide mandatory minimum information security requirements.

[39] GAO/AIMD-98-68.

Third, ensuring effective implementation of agency information security and CIP plans will require active monitoring by the agencies to determine whether milestones are being met and testing is being performed to determine whether policies and controls are operating as intended. With routine periodic evaluations, such as those required by GISRA and now FISMA, performance measurements can be more meaningful. In addition, the annual evaluation, reporting, and monitoring process established through these provisions is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.

Fourth, the Congress and the executive branch can use audit results, including the results of GISRA and FISMA reporting, to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. As highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. In our review of first-year GISRA implementation, we reported that many agencies emphasized the need for adequate funding to implement security requirements, and that security funding varied widely across the agencies. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, additional amounts are likely to be needed to address specific weaknesses and new tasks. At the same time, OMB and congressional oversight of future spending on information security will be important for ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk-management process. Further, we agree with OMB that much can be done to cost-effectively address common weaknesses, such as limited security training, across government rather than individually by agency.

Seventh, expanded research is needed in the area of information systems protection. Although a number of research efforts are under way, experts have noted that more is needed to achieve significant advances. In this regard, the Congress recently passed and the President signed into law the Cyber Security Research and Development Act to provide $903 million over 5 years for cybersecurity research and education programs.[40] This law directs the National Science Foundation to create new cybersecurity research centers, program grants, and fellowships. It also directs NIST to create new program grants for partnerships between academia and industry.

CIP Policy Has Continued to Evolve Since the Mid-1990s

CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are critical to national security, national economic security, and/or national public health and safety. Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Over the years, a variety of working groups has been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. The following sections summarize key developments in federal CIP policy to provide historical perspective.

President's Commission Studied Critical Infrastructure Protection

In October 1997, the President's Commission on Critical Infrastructure Protection issued a report[41] describing the potentially devastating implications of poor information security for the nation. The report recommended measures to achieve a higher level of CIP that included industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and a reconsideration of related laws. It further 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." The report also urged the FBI to continue its efforts to develop warning and threat analysis capabilities, which would enable it to serve as the preliminary national warning center for infrastructure attacks and to provide law

[40]P.L. 107-305, November 27, 2002.

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

enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

Presidential Decision Directive 63 Established Initial CIP National Strategy

In 1998, the President issued Presidential Decision Directive 63 (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 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, by 2003, have developed the ability to protect the nation's critical infrastructures from intentional destructive attacks.

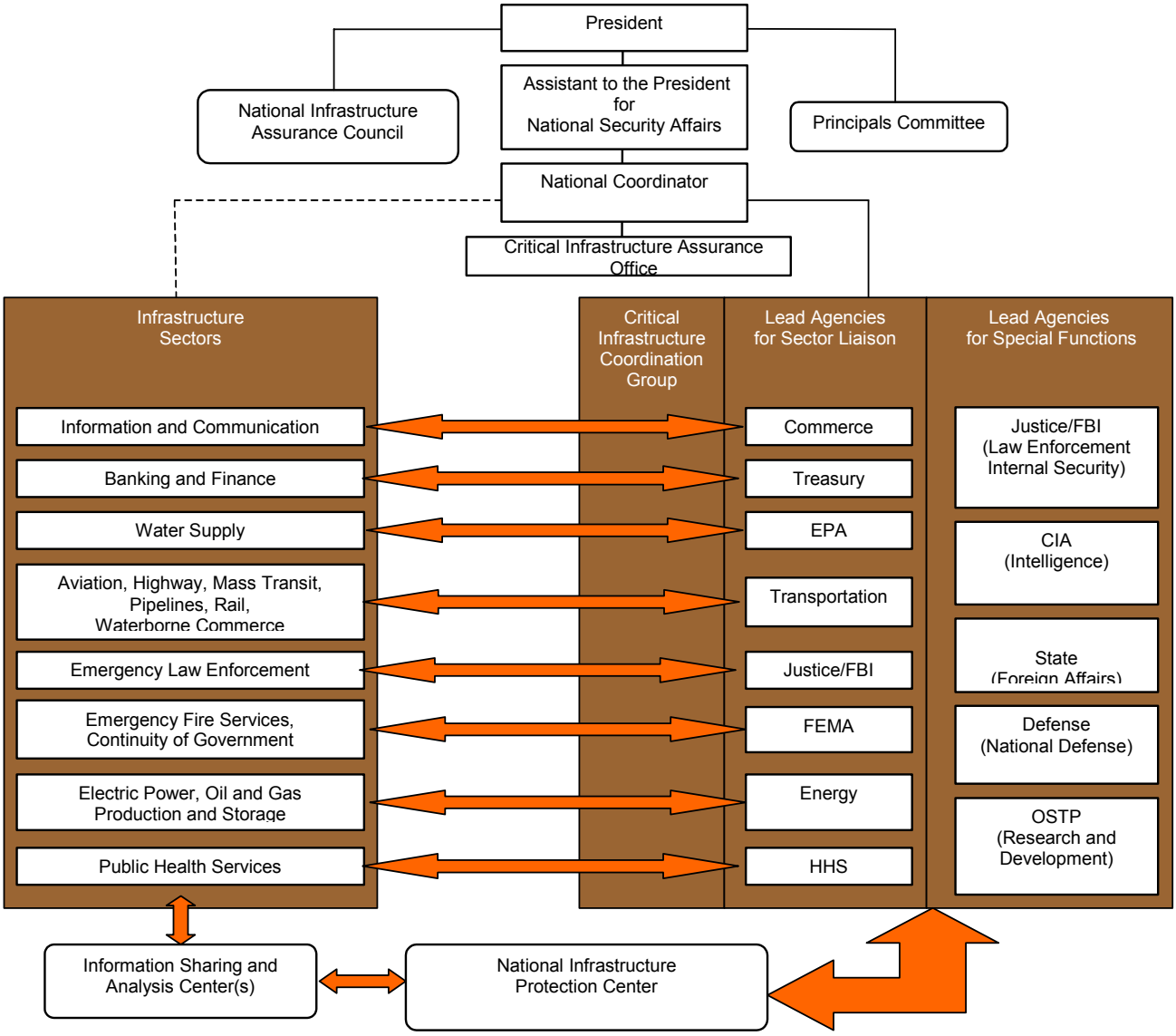
To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;
- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation/response; and
- the National Infrastructure Assurance Council (NIAC), which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. For each of the infrastuctures and functions, the directive designated lead federal agencies, referred to as sector liaisons, to work with their counterparts in the private sector, referred to as sector coordinators. To facilitate private-

sector participation, PDD 63 also encouraged the 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 through NIPC. Figure 3 displays a high-level overview of the organizations with CIP responsibilities, as outlined by PDD 63.

Figure 10: 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 Counter-terrorism and National Preparedness. In October 2001, Executive Order 13231 replaced the National Infrastructure Assurance Council with the National Infrastructure Advisory Council, and cyber CIP functions performed by the national coordinator were assigned to the chair of the President's Critical Infrastructure Protection Board. In February 2003, Executive Order 13231 was amended in its entirely by Executive Order 13286, dissolving the President's Critical Infrastructure Board and stating that the National Infrastructure Advisory Council chairpersons are to be selected from among its members.

PDD 63 called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. The sector liaison and the sector coordinator were to work with each other to address problems related to CIP for their sector. In particular, PDD 63 stated that they were to (1) develop and implement vulnerability awareness and education programs 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 rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

PDD 63 also required every federal department and agency to be responsible for protecting its own critical infrastructures, including both cyber-based and physical assets. To fulfill this responsibility, PDD 63 called for agencies' CIOs to be responsible for information assurance, and it required every agency to appoint a chief infrastructure assurance officer to be responsible for the protection of all other aspects of an agency's critical infrastructure. Further, it required federal agencies to:

- develop, implement, and periodically update a plan for protecting its critical infrastructure;
- determine its minimum essential infrastructure that might be a target of attack;
- conduct and periodically update vulnerability assessments of its minimum essential infrastructure;
- develop a recommended remedial plan based on vulnerability assessments 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.

National Plan for Information Systems Protection Provided Plan for Federal Government

In January 2000, the White House issued its National Plan for Information Systems Protection.[42] 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 of 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.

Executive Order 13228 Established the Office of Homeland Security

In October 2001, the President issued Executive Order (EO) 13228,[43]establishing the Office of Homeland Security within the Executive Office of the President and the Homeland Security Council. It stated that the Office of Homeland Security was "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." In addition, EO 13228 stated that, among other things, the Office of Homeland Security was to coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attacks. Further, it established the Homeland Security Council to advise and assist the President with respect to all aspects of homeland security, to serve as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies, and to develop and implement homeland security policies.

[42]The 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).

[43]"Establishing the Office of Homeland Security and the Homeland Security Council," Executive Order 13228, Oct. 8, 2001.

Executive Order 13231 Established the CIP Board

In October 2001, President Bush signed EO13231, establishing the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures. Executive Order 13231 tasked the board with recommending policies and coordinating programs for protecting CIP-related information systems. The Special Advisor to the President for Cyberspace Security chaired the board. The executive order also established 10 standing committees to support the board's work on a wide range of critical information. According to EO 13231, the board's responsibilities were to recommend policies and coordinate programs for protecting information systems for critical infrastructures, including emergency preparedness communications and the physical assets that support such systems. The Special Advisor reported to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security and coordinated 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.

National Strategy for Homeland Security Included CIP Components

In July 2002, the President issued the *National Strategy for Homeland Security*, with strategic objectives to (1) prevent terrorist attacks within the United States, (2) reduce America's vulnerability to terrorism, and (3) minimize the damage and recovery from attacks that do occur. To ensure coverage of critical infrastructure sectors, this strategy identified 13 industry sectors, expanded from the 8 originally identified in PDD 63, as essential to our national security, national economic security, and/or national public health and safety. Lead federal agencies were identified and directed to work with their counterparts in the private sector to assess sector vulnerabilities and to develop plans to eliminate vulnerabilities. The sectors and their lead agencies are listed in table 2.

Table 2: 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 National Strategy to Secure Cyberspace

The Homeland Security Act Created the Department of Homeland Security

The Homeland Security Act of 2002 (signed by the President on November 25, 2002) established the Department of Homeland Security (DHS). 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 created the Information Analysis and Infrastructure Protection Directorate within the new department and transferred 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 the CIAO.

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 the comprehensive national infrastructure protection plan. Such a plan was subsequently

required by the Homeland Security Act of 2002. 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*.[44] These two strategies identify priorities, actions, and responsibilities for the federal government, including lead agencies and DHS, as well as for state and local governments and the private sector.

The National Strategy to Secure Cyberspace Provided Initial Framework for Cyber CIP

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. The strategy reiterates the critical infrastructure sectors and the related lead federal agencies as identified in *The National Strategy for Homeland Security*. In addition, the strategy identifies DHS as the central coordinator for cyberspace efforts. As such, DHS is responsible for coordinating and working with other federal entities involved in 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**—Coordinated by DHS, this system is described as a public/private architecture 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 to 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 DHS in coordinating crisis management for cyberspace security; coordinating processes for voluntary public/private participation in the development of national public/private continuity and contingency plans; exercising

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

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 and supervisory control and data acquisition 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 promoting 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 Governments' Cyberspace**—To help protect, improve, and maintain governments' 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 to 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 Provided National Policy for Physical CIP

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. Although the strategy does not explicitly mention PDD 63, it builds on the directive with its sector-based approach that includes the 13 sectors defined in the *National Strategy for Homeland Security*, identifies federal departments and agencies as sector liaisons, and calls for expanding the capabilities of ISACs. The strategy is based on eight guiding principles, including 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 assure 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 assure the protection of infrastructures and assets facing specific, imminent threats; and the third is to pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time. Under this strategy, DHS will provide overall cross-sector coordination and serve as the primary liaison and facilitator for cooperation among federal agencies, state and local governments, and the private sector. The strategy states that the private sector generally remains the first line of defense for its own facilities and should reassess and adjust their planning, assurance, and investment programs to better accommodate the increased risk presented by deliberate acts of violence. 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.

Executive Order 13286 Reflected Establishment of DHS

On February 28, 2003, Executive Order (EO) 13231 was amended in its entirety by Executive Order 13286.[45] Although EO 13286 maintained the same national policy statement regarding the protection against disruption of information systems for critical infrastructures, it dissolved the President's Critical Infrastructure Protection Board that was to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures, and the board's chair— the Special Advisor to the President for Cyberspace Security—and related staff, along with the 10 standing committees established to support the board's work on a wide range of critical information infrastructure efforts. According to EO 13286, the NIAC is to continue to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy. However, NIAC will provide its advice through the Secretary of Homeland Security. Regarding the functions of the standing committees, an OMB official stated that OMB will continue to oversee the federal information security committee functions. Further, recent media reports state that efforts are underway to ensure the transition of certain other functions to DHS.

Other Developments

On March 1, 2003, DHS assumed certain essential information and analysis and infrastructure protection functions and organizations, including NIPC (other than the Computer Investigation and Operations Section) and the CIAO. Currently, according a Department of Homeland Security official, the department is continuing to carry out the activities previously performed by NIPC and the other transferred functions and organizations. Further, the official stated that the department is enhancing those activities as they are integrated within the new department and are developing a business plan. The DHS official stated that the department is continuing previously established efforts to maintain and build relationships with other federal entities, including the FBI and other NIPC partners, and with the private sector. In addition, the department plans to provide staff to work at the proposed Terrorist Threat Integration Center. Although NIPC experienced the loss of certain senior leadership prior to transition to the new department and have identified some staffing needs, the DHS official stated that the department is able to provide the functions previously performed by NIPC.

[45]The White House, Executive Order 13286—Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security (Washington, D.C.: Feb. 28, 2003).

The Nation Faces Ongoing CIP Challenges

Although the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, we have made numerous recommendations over the last several years concerning CIP challenges that still need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, even greater efforts are needed to address them. These challenges include developing a comprehensive and coordinated national CIP plan, improving information sharing on threats and vulnerabilities, improving analysis and warning capabilities, and ensuring appropriate incentives to encourage entities outside of the federal government to increase their CIP efforts. It is also important that CIP efforts be appropriately integrated with DHS.

A Comprehensive and Coordinated National CIP Plan Needs to Be Developed

An underlying issue in the implementation of CIP is that no national plan yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures. Such a clearly defined plan is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. Since 1998, we have reported on the need for such a plan and made numerous related recommendations.

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of federal entities was important to ensure governmentwide cooperation and support for PDD 63.[46] At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures.

[46]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).

However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives were to be met, as well as guidelines for measuring progress.[47] Accordingly, we made several recommendations to supplement those we had made in the past. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in CIP and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

In July 2002 we issued a report identifying at least 50 organizations that were involved in national or multinational cyber CIP efforts, including 5 advisory committees, 6 Executive Office of the President organizations, 38 executive branch organizations associated with departments, agencies, or intelligence organizations, and 3 other organizations.[48] Although our review did not cover organizations with national physical CIP responsibilities, the large number of organizations that we did identify as involved in CIP efforts presents a need to clarify how these entities coordinate their activities with each other. Our report also stated that PDD 63 did not specifically address other possible critical sectors and their respective federal agency counterparts. Accordingly, we recommended that the federal government's strategy also

- include all relevant sectors and define the key federal agencies' roles and responsibilities associated with each of these sectors, and

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

[48]U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

- define the relationships among the key CIP organizations.

In July 2002, the *National Strategy for Homeland Security* called for interim cyber and physical infrastructure protection plans that DHS would use to build a comprehensive national infrastructure plan. According to the *National Strategy for Homeland Security*, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local government and the private sector. The plan is to establish standards and benchmarks for infrastructure protection and provide a means to measure performance. The strategy also states that DHS is to unify the currently divided responsibilities for cyber and physical security. In November 2002, as mentioned previously, the Homeland Security Act of 2002 created DHS and, among other things, required it to develop a comprehensive national plan.

In February 2003, the President issued the interim strategies—*The National Strategy to Secure Cyberspace and The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereafter referred to in this testimony as the cyberspace security strategy and the physical protection strategy). Both define strategic objectives for protecting our nation's critical assets. These strategies identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and DHS, as well as for state and local governments and the private sector. The two do not (1) clearly indicate how the physical and cyber efforts will be coordinated; (2) define the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicate time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; or (4) establish performance measures for which entities can be held responsible. Until a comprehensive and coordinated plan is completed that unifies the responsibilities for cyber and physical infrastructures; identifies roles, responsibilities, and relationships for all CIP efforts; establish time frames or milestones for implementation; and establishes performance measures, our nation risks not having a consistent and appropriate framework to deal with growing threats to its critical infrastructure.

Better Information Sharing on Threats and Vulnerabilities Must Be Implemented

Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we have reported in recent years, establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult. In addition, the private sector has expressed concerns about sharing information with the government and the difficulty of obtaining security clearances.

In October 2001, we reported on information sharing practices that could benefit CIP.[49] These practices include

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory changes.

A number of activities have been undertaken to build relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish ISACs. For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members include representatives from private industry, other government agencies, state and local law enforcement, and the academic community. As of February 2003, InfraGard members totaled over 6,700.

[49]U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

As stated above, PDD 63 encouraged the voluntary creation of ISACs to serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. ISACs are critical since private-sector entities control over 80 percent of our nation's critical infrastructures. Their activities 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.

While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities which the ISACs could undertake, including:

- establishing baseline statistics and patterns on the various infrastructures;
- serving as a clearinghouse for information within and among the various sectors;
- providing a library for historical data for use by the private sector and government; and
- reporting private-sector incidents to NIPC.

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. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us in July 2002 that an ISAC development and support unit had been created, whose mission was to enhance private-sector cooperation and trust so that it would result in a two-way sharing of information. DHS now reports that there are currently 16 ISACs, including ISACs established for sectors not identified as critical infrastructure sectors. Table 3 lists the current ISACs identified by DHS and the lead agencies. DHS officials stated that they have formal agreements with most of the current ISACs.

Table 3: Lead Agencies and ISAC Status by CIP Sector

Sectors	Designated lead agency	ISAC established
Sectors Identified by PDD 63		
Information and telecommunications	Homeland Security*	
Information technology		✓
Telecommunications		✓
Banking and finance	Treasury	✓
Water	Environmental Protection Agency	✓
Transportation	Homeland Security*	
Aviation		
Surface Transportation		✓
Maritime		prospective
Trucking		✓
Emergency Services**	Homeland Security*	
Emergency law enforcement		✓
Emergency fire services		✓
Government **		
Interstate		✓
Energy	Energy	
Electric power		✓
Oil and gas		✓
Public health	Health and Human Services	
Sectors identified by *The National Strategy for Homeland Security*		
Food		✓
Meat and poultry	Agriculture	
All other food products	Health and Human Services	
Agriculture	Agriculture	
Chemical industry and hazardous materials	Environmental Protection Agency	
Chemicals		✓
Defense industrial base	Defense	
Postal and shipping	Homeland Security	
National monuments and icons	Interior	
Other Sectors that have established ISACs		
Research and Education Networks		✓
Real Estate		✓

*The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigation, and the Federal Emergency Management Agency.

**PDD 63 identified as critical sectors (1) emergency law enforcement and (2) emergency fire services and continuity of government. In the new National Strategy for Homeland Security, emergency law enforcement and emergency fire services are both included in an emergency services sector. Also, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.

In spite of progress made in establishing ISACs, additional efforts are needed. All sectors do not have a fully established ISAC, and of those sectors that do, there is mixed participation. The amount of information being shared between the federal government and private-sector organizations also varies. Specifically, the five ISACs we recently reviewed[50] showed different levels of progress in implementing the PDD 63 suggested activities. Specifically, four of the five reported that efforts to establish baseline statistics were still in progress. Also, while all five reported that they serve as the clearinghouse for their own sectors, only three of the five reported that they are also coordinating with other sectors. Only one of the five ISACs reported that it provides a library of incidents and historical data that is available to both the private sector and the federal government, and although three additional ISACs do maintain a library, it is available only to the private sector. The one remaining ISAC reported that they had yet to develop a library but have plans to do so. Finally, four of the five stated that they report incidents to NIPC on a regular basis.

Some in the private sector have expressed concerns about voluntarily sharing information with the government. Specifically, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. For example, neither the information technology nor the energy or the water ISACs share their libraries with the federal government because of concerns that information could be released under FOIA. And, officials of the energy ISAC stated that they have not reported incidents to NIPC because of FOIA and antitrust concerns.

Other obstacles to information sharing, previously mentioned in congressional testimony, include difficulty obtaining security clearances for ISAC personnel and the reluctance to disclose corporate information. In July 2002 congressional testimony, the Director of Information Technology for the North American Electric Reliability Council stated that the owners of critical infrastructures need access to more specific threat

[50]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

information and analysis from the public sector and that this may require either more security clearances or declassifying information.[51]

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities 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. The *National Strategy for Homeland Security*, which outlines 12 major legislative initiatives, includes "enabling critical infrastructure information sharing." It 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. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and the private sector.

Actions have already been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.[52] Moreover, the 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 DHS. These restrictions include 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 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.

[51]Testimony of Lynn P. Constantini, Director, Information Technology, North American Electric Reliability Council, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2002.

[52]The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), Public Law No. 107-56, October 26, 2001.

Information sharing within the government also remains a challenge. In April 2001, we reported that NIPC and other government entities had not developed fully productive information sharing and cooperative relationships.[53] For example, federal agencies had not routinely reported incident information to NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's FedCIRC. Further, NIPC and DOD officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. The NIPC director stated in July 2002 that the relationship between NIPC and other government entities had significantly improved since our review, and the quarterly meetings with senior government leaders were instrumental in improving information sharing. In addition, in testimony subsequent to our work, officials from the FedCIRC and the U.S. Secret Service discussed the collaborative and cooperative relationships that had since been formed between their agencies and NIPC.

The private sector has also expressed its concerns about the value of information being provided by the government. For example, in July 2002 the President for the Partnership for Critical Infrastructure Security stated in congressional testimony that information sharing between the government and private sector needs work, specifically, in the quality and timeliness of cyber security information coming from the government.[54]

The cyberspace security strategy reiterates that the federal government encourages the private sector to continue to establish ISACs and to enhance the analytical capabilities of existing ISACs. It states that ISACs will play an increasingly important role in the national cyberspace security response system and the overall missions of homeland security. In addition, the physical protection strategy states that the overall management of information sharing activities among government agencies

[53]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 24, 2001).

[54]Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security, before the Subcommittee on Oversight and Investigation of the Energy and Commerce Committee, U.S. House of Representatives, July 9, 2002.

and between public and private sectors has lacked proper coordination and facilitation. The physical protection strategy also establishes specific initiatives for creating more effective and efficient information sharing, including defining protection-related information sharing requirements and promoting the development and operation of critical sector ISACs, and implementing the statutory authorities and powers of the Homeland Security Act of 2002.

Analysis and Warning Capabilities Need to Be Improved

Another key CIP challenge is to develop more robust analysis and warning capabilities to identify threats and provide timely warnings, including an effective methodology for strategic analysis and a framework for collecting needed threat and vulnerability information. Such capabilities need to address both cyber and physical threats.

NIPC was established in PDD 63 as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is under way or imminent. Similar activities are also called for in DHS's Information Analysis and Infrastructure Protection Directorate, which has absorbed NIPC.

In April 2001, we reported on NIPC's progress in developing national capabilities for analyzing threat and vulnerability data, issuing warnings, and responding to attacks, among other issues.[55] Overall, we found that while progress in developing these capabilities was mixed, NIPC had initiated a variety of CIP efforts that had laid a foundation for future governmentwide efforts. In addition, NIPC had provided valuable support and coordination related to investigating and otherwise responding to

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

attacks on computers. However, at the close of our review, the analytical capabilities that PDD 63 asserted were needed to protect the nation's critical infrastructures had not yet been achieved, and NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

At the time of our review, NIPC had issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. In addition, it had issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis. We reported that the use of strategic analysis to determine the potential broader implications of individual incidents had been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

We also reported that three factors hindered NIPC's ability to develop strategic analytical capabilities:[56]

- First, there was no generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.

- Second, NIPC had sustained prolonged leadership vacancies and did not have adequate staff expertise, in part because other federal agencies had not provided the originally anticipated number of detailees. For example, at the close of our review in February 2001, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of NIPC's 3-year existence. In addition, NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimated were needed to develop analytical capabilities.

[56] GAO-01-323.

- Third, NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work, only three industry assessments had been partially completed, and none had been provided to NIPC. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

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

  In addition, NIPC's own plans for further developing its analysis and warning capabilities were fragmented and incomplete. The relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council were unclear regarding who had direct authority for setting NIPC priorities and procedures and providing NIPC oversight. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

  In our report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;

- require the development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and

- clearly define the role of NIPC in relation to other government and private-sector entities.

In July 2002, NIPC's director stated that, in response to our report's recommendations, NIPC had developed a plan with goals and objectives to improve its analysis and warning capabilities and had made considerable progress in this area. The plan establishes and describes performance measures both for its analysis and warning section and for other issues relating to staffing, training, investigations, outreach, and warning. In addition, the plan describes the resources needed to reach the specific goals and objectives for the analysis and warning section. The director also stated that the analysis and warning section had created two additional teams to bolster its analytical capabilities: (1) the critical infrastructure assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community. The director added that NIPC (1) started holding a quarterly meeting with senior government leaders of entities that it regularly works with to better coordinate its analysis and warning capabilities; (2) had developed close working relationships with other CIP entities involved in analysis and warning activities, such as FedCIRC, DOD's Joint Task Force for Computer Network Operations, Carnegie Mellon's CERT Coordination Center, and the intelligence and anti-virus communities; and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation.

The director also stated in July 2002 that NIPC had received sustained leadership commitment from key entities, such as the CIA and the National Security Agency, and that it continued to increase its staff primarily through reservists and contractors. However, the director acknowledged that our recommendations were not fully implemented and that despite the accomplishments to date, much more had to be done to create the robust analysis and warning capabilities needed to adequately address cyberthreats.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been focused on cyber threats. In April 2001, we reported that while PDD 63 covers both physical and computer-based threats, federal efforts to meet the directive's requirements have pertained primarily to computer-based threats, since this was an area that the leaders of the administration's CIP strategy view as needing attention. In July 2002, NIPC reported that the potential for concurrent cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. In July 2002, the director of NIPC told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC had developed thresholds with several ISACs for reporting physical incidents and, since January 2002, has issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability will be a significant challenge. The physical protection strategy states that DHS will maintain a comprehensive, up to date assessment of vulnerabilities across sectors and improve processes for domestic threat data collection, analysis, and dissemination to state and local government and private industry.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities. For example, there has been considerable public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, as the transfer of NIPC to DHS organizationally separated NIPC from the FBI's law enforcement activities, including the Counterterrorism Division and NIPC field agents, it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the new DHS are effective and that appropriate information is exchanged on a timely basis.

In January 2003, the President announced the creation of a multi-agency Terrorist Threat Integration Center (TTIC) to merge and analyze terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture. The center will be formed from elements of the Department of Homeland Security, the FBI's

Counterterrorism Division, the Director of Central Intelligence's Counterterrorist Center, and the Department of Defense.[57] Specifically, the President stated that it would:

- optimize the use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;
- create a structure that ensures information sharing across agency lines in a way consistent with our national values of privacy and civil liberties;
- integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture; and
- be responsible and accountable for providing terrorist threat assessments for our national leadership.

The TTIC is scheduled to begin operations within the CIA's facilities on May 1, 2003, but will eventually move to a new, independent facility. The center is to receive $50 million in fiscal year 2004. The TTIC will fuse international threat-related information from the CIA with domestic threat-related information collected by the FBI's Joint Terrorism Task Forces and analyzed by a separate FBI information-analysis center.

In addition, according to NIPC's director, as of July 2002, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI testified in June 2002 that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds require a centralized and robust analytical capacity that did not exist in the FBI's Counterterrorism Division.[58] He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations requires an enhanced analytical and data mining capacity that was not then available. Furthermore, NIPC's director stated that multiagency staffing, similar to NIPC, is a critical

[57]The White House, *Fact Sheet: Strengthening Intelligence to Better Protect America* (Washington, D.C.: Jan. 28, 2003).

[58]Testimony of Robert S. Mueller, III, Director Federal Bureau of Investigation, before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives, June 21, 2002.

success factor in establishing an effective analysis and warning function and that appropriate funding for such staff is important.

The *National Strategy for Homeland Security* identified intelligence and warning as one of six critical mission areas and called for major initiatives to improve our nation's analysis and warning capabilities. The strategy also stated that no government entity was then responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. The Homeland Security Act gives such responsibility to the new DHS. Further, the Act gives DHS broad statutory authority to access intelligence information, as well as other information, relevant to the terrorist threat and to turn this information into useful warnings. For example, according to a White House fact sheet, DHS's Information Analysis and Infrastructure Protection Directorate is to receive and analyze terrorism-related information from the TTIC.[59]

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The President's *National Strategy for Homeland Security* also stated that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy stated that the U.S. government does not perform vulnerability assessments of the nation's entire critical infrastructure. The Homeland Security Act of 2002 stated DHS's Under Secretary for Information Analysis and Infrastructure Protection is to carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructures of the United States.

Additional Incentives Are Needed to Encourage Increased Nonfederal Efforts

The President's fiscal year 2004 budget request for the new DHS includes $829 million for information analysis and infrastructure protection, a significant increase from the estimated $177 million for fiscal year 2003. In particular, the requested funding for 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.

[59]The White House, *Fact Sheet: Strengthening Intelligence to Better Protect America* (Washington, D.C.: Jan. 28, 2003).

Although 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, additional incentives may still be needed to encourage nonfederal entities to increase their CIP efforts.

PDD 63 also stated that sector liaisons should identify and assess economic incentives to encourage the desired sector behavior in CIP. Further, to facilitate private-sector participation, it encouraged the voluntary creation of information sharing and analysis centers (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. Consistent with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use policy tools to protect the health, safety, or well-being of the American people. It mentions federal grants programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The physical security strategy reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets. The cyberspace security strategy also states that the market is to provide the major impetus to improve cyber security and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on 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.[60] We have previously testified on the choice and design of public policy tools that are available to governments.[61] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address

[60]U.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).

[61]U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness* Strategy, GAO-02-549T (Washington, D.C.: Mar. 28, 2002).

security concerns. Some of these tools are already being used. For example, as the lead agency for the water sector, the EPA reported providing approximately 449 grants totaling $51 million to assist large drinking water utilities in developing 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 as a condition for membership that its members perform enhanced security activities, including vulnerability assessments. However, because a significant percentage of companies that operate major hazardous chemical facilities do not perform these voluntary security activities, the physical security strategy recognized that mandatory measures may be required. The strategy stated that EPA, in consultation with DHS and other federal, state, and local agencies, will review current laws and regulations pertaining to the sale and distribution of highly toxic substances to determine whether additional measures are necessary. Moreover, the strategy also stated that DHS, in concert with EPA, will work with Congress to enact legislation requiring certain facilities, particularly those that maintain large quantities of hazardous chemicals in close proximity to large populations, to enhance site security.

Without appropriate consideration of public policy tools, private sector participation in sector-related CIP efforts may not reach its full potential. For example, we reported in January 2003 on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sectorwide efforts. We also reported on the efforts of federal entities and regulators to partner with the financial services industry to protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the potential public policy tools to encourage the financial services sector in implementing CIP-related efforts. Because of the importance of considering public policy tools to encourage private sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress five ISACs had made in accomplishing the activities suggested by PDD 63. We recommended that the responsible lead agencies assess of the need for 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.

In summary, through audit and evaluation results and the management review and reporting requirements implemented through GISRA and now FISMA, agencies have increased management attention to information security and begun to show progress in correcting identified weaknesses. In addition, continued guidance and OMB and congressional oversight have emphasized the ongoing commitment to improving the federal government's information security. Such efforts must be sustained to help ensure that federal agencies are responding to and providing appropriate protections against the growing threat to the systems that support their missions and provide vital services to the American people. Further, we believe that a comprehensive strategy addressing certain key issues would help to guide these efforts and ensure that they are coordinated and consistently implemented governmentwide.

Over the last several years, we have also identified various challenges to the implementation of CIP that need to be addressed. Although improvements have been made and continuing efforts are in progress, greater efforts are still needed to effectively address them. These challenges include developing a comprehensive and coordinated national plan, improving information sharing on threats and vulnerabilities between the private sector and the federal government as well as within the government itself, improving analysis and warning capabilities, and encouraging entities outside the federal government to increase CIP efforts. It is also important to emphasize that much of the success of ensuring the security of our nation's critical infrastructure will depend on appropriately integrating all CIP efforts with the implementation of the new DHS.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time. If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by E-mail at daceyr@gao.gov.