United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Wednesday,
September 26, 2001

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks

Statement of Joel C. Willemssen
Managing Director, Information Technology Issues

G A O
Accountability * Integrity * Reliability

GAO-01-1168T

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts to protect federal agency information systems and our nation's critical computer-dependent infrastructures. Federal agencies, and other public and private entities, rely extensively on computerized systems and electronic data to support their missions. 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, as the Comptroller General stated in testimony last week, protecting against computer-based attacks on critical infrastructures is an important aspect of homeland security.[1]

Today, I will provide an overview of our recent reports on federal information security and critical infrastructure protection. Specifically, I will summarize the pervasive nature of federal system weaknesses, outline the serious risks to federal operations, and then detail the specific types of weaknesses identified at federal agencies. I will also discuss the importance of establishing a strong agencywide security management framework and how new evaluation and reporting requirements can improve federal efforts. Next, I will provide an overview of the strategy described in Presidential Decision Directive (PDD) 63 for protecting our nation's critical infrastructures from computer-based attacks. Finally, I will summarize the results of our recent evaluation of progress in implementing PDD 63, which was issued last week as part of a broader evaluation of federal counterterrorism efforts.[2] My summary of PDD 63 progress will also cover the results of our April report on the National Infrastructure Protection Center (NIPC), an interagency center housed in the Federal Bureau of Investigation (FBI), which is responsible for providing analysis, warning, and response capabilities for combating computer-based attacks.[3]

[1] *Homeland Security: A Framework for Addressing the Nation's Efforts* (GAO-01-1158T, September 21, 2001).

[2] *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

[3] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

Results in Brief

Because of our government's and our nation's reliance on interconnected computer systems to support critical operations and infrastructures, poor information security could have potentially devastating implications for our country. Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems have significant pervasive weaknesses that continue to put critical operations and assets at risk. In particular, federal agencies continue to have deficiencies in their entitywide security programs that are critical to their success in ensuring that risks are understood and that effective controls are selected and implemented. The new statutory government information security reform provisions will be a major catalyst for federal agencies to improve their security program management. To help maintain the momentum that these provisions have generated, agencies must act quickly to implement strong security program management.

An array of efforts has been undertaken to implement the national critical infrastructure protection strategy outlined in PDD 63. However, progress in certain key areas has been limited. Outreach efforts by numerous federal entities to establish cooperative relationships with and among private and other nonfederal entities have raised awareness and prompted information sharing. However, efforts to perform substantive analyses of sector-wide and cross-sector interdependencies and related vulnerabilities have been limited. In addition, federal agencies have taken initial steps to develop critical infrastructure protection plans; but, as mentioned above, significant weaknesses continue to be identified in their computer-based controls. Further, although the NIPC has initiated a variety of critical infrastructure protection efforts that have laid a foundation for future governmentwide efforts, it has not developed the analytical and information-sharing capabilities that PDD 63 asserted are needed. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

A major impediment to implementing the strategy outlined in PDD 63 is the lack of a national plan that clearly delineates the roles and responsibilities of federal and nonfederal entities and defines interim objectives. In our report on combating terrorism, issued last week, we recommended that the Assistant to the President for National Security Affairs ensure that a more fully defined strategy to address computer-based threats be developed that addresses this impediment. It will be important that this strategy be coordinated with the counterterrorism efforts undertaken by the newly established Office of Homeland Security.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing 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 on a 24-hour-a-day basis; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with virtually an unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services all depend on the security of their computer operations. Likewise, the speed and accessibility that create the enormous benefits of the computer age, 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.

Reports of attacks and disruptions are growing. The number of computer security incidents reported to the CERT Coordination Center® (CERT-CC)[4] rose from 9,859 in 1999 to 21,756 in 2000. For the first 6 months of 2001, 15,476 incidents were reported. 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 potential hacker can literally download tools from the Internet and "point and click" to start a hack. According to a recent National Institute of Standards and Technology publication, hackers post 30 to 40 new tools to hacking sites on the Internet every month.

Recent attacks over the past 2 months illustrate the risks. These attacks, referred to as Code Red, Code Red II, and SirCam, have affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. They have already reportedly caused billions of dollars of damage, and their full effects have yet to be completely assessed. Code Red attacks have reportedly

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

(1) caused the White House to change its website address, (2) forced the Department of Defense (DOD) to briefly shut down its public websites, (3) infected Treasury's Financial Management Service, causing it to disconnect its systems from the Internet, (4) caused outages for users of Qwest's high-speed Internet service nationwide, and (5) delayed FedEx package deliveries. Our testimony last month provides further details on the nature and impact of these attacks.[5]

More recently, the Nimda worm uses some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus, allowing it to spread widely in a short amount of time. This worm modifies web documents (for example, .htm and .html files) and certain executable files found on the systems it infects, and creates numerous copies of itself under various file names. It also may create a denial of service as a result of network scanning and email propagation.

These are just the latest episodes. The cost of last year's ILOVEYOU virus is now estimated to be more than $8 billion. Other incidents reported in 2001 illustrate the problem further:

- A hacker group by the name of "PoizonB0x" defaced numerous government web sites, including those of the Department of Transportation, the Administrative Office of the U.S. Courts, the National Science Foundation, the National Oceanic and Atmospheric Administration, the Princeton Plasma Physics Laboratory, the General Services Administration, the U.S. Geological Survey, the Bureau of Land Management, and the Office of Science and Technology Policy. (Source: Attrition.org., March 19, 2001.)
- The "Russian Hacker Association" offered over the Internet an e-mail bombing system that would destroy a person's "web enemy" for a fee. (Source: UK Ministry of Defense Joint Security Coordination Center.)

Even before the tragic events of September 11, government officials were 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, or degrade

[5] *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* (GAO-01-1073T, August 29, 2001).

the integrity of and deny access to data.[6] 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, the likelihood that information attacks will threaten vital national interests increases. In addition, the disgruntled organization insider is a significant threat, since such individuals with little knowledge about computer intrusions often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets. Since September 11, the NIPC has warned of an expected upswing in incidents and encouraged system administrators to follow best practices to limit the potential damage from any cyber attacks. In particular, the NIPC warned against political hacking by self-described "patriot" hackers targeted at those perceived to be responsible for the terrorist attacks as well as virus propagation, in which old viruses are renamed to appear related to recent events.

Weaknesses in Federal Systems Remain Pervasive

Since 1996, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September 1996, we reported that serious weaknesses had been found at 10 of the 15 largest federal agencies, and we concluded that poor information security was a widespread federal problem with potentially devastating consequences.[7] In 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies; both analyses found that all 24 agencies had significant

[6]These terms are defined as follows: *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 bombs*: 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.

[7]*Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

information security weaknesses.[8] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[9]

Our most recent analysis, last April, of reports published since July 1999, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[10] Weaknesses continued to be reported in each of the 24 agencies covered by our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented, (2) access controls, which ensure that only authorized individuals can read, alter, or delete data, (3) software development and change controls, which ensure that only authorized software programs are implemented, (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection, (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse, and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

Our April analysis 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.

---

[8] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998) and *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

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

[10] *Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk* (GAO-01-600T, April 5, 2001).

Most of the audits covered in our analysis 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 systems supporting nonfinancial operations. In response to congressional interest, since fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations. We expect this trend to continue.

Risks to Federal Operations are Substantial

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 of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections, and weaknesses at DOD increase the vulnerability of various military operations. Further, information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure. For example, in 1999, a Social Security Administration employee pled guilty to unauthorized access to the administration's systems. The related investigation determined that the employee had made many unauthorized queries, including obtaining earnings information for members of the local business community.

More recent audits in 2001 show that serious weaknesses continue to be a problem and that critical federal operations and assets remain at risk.

- In August, we reported that significant and pervasive weaknesses placed Commerce's systems at risk. Many of these systems are considered critical

to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.[11] Also, Commerce's inspector general has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.[12]

- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than $12 billion annually in payments that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.[13]

- In March, we reported that although the DOD's Department-wide Information Assurance Program had made progress in addressing information assurance, it had not yet met its goals of integrating information assurance with mission readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.[14]

- In February, the Department of Health and Human Services' Inspector General again reported serious control weaknesses affecting the integrity,

[11] *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk* (GAO-01-751, August 13, 2001).

[12] Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements, Inspector General Audit Report No. FSD-12849-1-0001.

[13] *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk* (GAO-01-615, July 3, 2001).

[14] *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, March 30, 2001).

confidentiality, and availability of data maintained by the department.[15] Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which was responsible, during fiscal year 2000, for processing more than $200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data, such as Medicare enrollment, eligibility and paid claims data, and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

These types of risks, if inadequately addressed, may limit the government's ability to take advantage of new technology and improve federal services through electronic means. For example, this past February, we reported on serious control weaknesses in the Internal Revenue Service's (IRS) electronic filing system, noting that failure to maintain adequate security could erode public confidence in electronic filing, jeopardize the Service's ability to meet its goal of 80 percent of returns being filed electronically by 2007, and deprive it of financial and other anticipated benefits.

Specifically, we found that, during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both within and outside IRS, could have gained access to these systems and viewed, copied, modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electronic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS completed corrective action for all the critical access control vulnerabilities we identified before the 2001 filing season and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.[16] As part of our audit follow up activities, we plan to evaluate the effectiveness of IRS' corrective actions.

Addressing weaknesses such as those we identified in the IRS's electronic filing system is especially important in light of the administration's plans to improve government services by expanding use of the Internet and other computer-facilitated operations—collectively referred to as

[15] *Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000*, A-17-00-00014, February 26, 2001.

[16] *Information Security: IRS Electronic Filing Systems* (GAO-01-306, February 16, 2001).

electronic government, or E-government.[17] Specific initiatives proposed for fiscal year 2002 include expanding electronic means for (1) providing information to citizens, (2) handling procurement-related transactions, (3) applying for and managing federal grants, and (4) providing citizens information on the development of specific federal rules and regulations. Anticipated benefits include reducing the expense and difficulty of doing business with the government, providing citizens improved access to government services, and making government more transparent and accountable. Success in achieving these benefits will require agencies and others involved to ensure that the systems supporting E-government are protected from fraud, inappropriate disclosures, and disruption. Without this protection, confidence in E-government may be diminished, and the related benefits never fully achieved.

Control Weaknesses Across Agencies are Similar

Although the nature of agency operations and their related risks vary, striking similarities remain in the specific types of general control weaknesses reported and in their serious adverse impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. Likewise, similarities exist in the corrective actions they must take. The following sections describe the six areas of general controls and the specific weaknesses that have been most widespread at the agencies covered by our analysis.

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost effective manner rather than reacting to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed

[17]The President's Management Agenda, Fiscal Year 2002, www.whitehouse.gov/omb/budget.

security plans for major systems based on risk (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on ineffective controls, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they execute. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Also, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and departing employees, as well as changes in users' responsibilities and related access needs.

Significant access control weaknesses were reported for all the agencies covered by our analysis, as shown by the following examples:

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled nor were they adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, at one agency, former employees and contractors could still and in many cases did read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.
- Users were not required to periodically change their passwords.
- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At another agency, 20,000 users had been provided access to one system without written authorization.
- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the ability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also, at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate network vulnerability testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. Our auditors have been successful, in almost every test, in readily gaining unauthorized access that would allow both internal and external intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. Also, much of the activity associated with our intrusion testing has not been recognized and recorded, and the problem

reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Software Development and Change Controls

Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and ensure that different versions are not misidentified.

Such controls can prevent errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that, depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Weaknesses in software program change controls were identified for almost all the agencies for which these controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. At another agency, documentation was not retained to demonstrate user testing and acceptance.
- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs was prevented or detected.
- Agencies' policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or
- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Segregation of duties can be enforced by a combination of physical and logical access controls and by effective supervisory review. We identified weaknesses in segregation of duties at most agencies covered by our analysis. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff members involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 staff members had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year

1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt-recorded by the same individual.

Operating System Software Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosure. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. Weaknesses were identified at each agency for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have

engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Further, pervasive vulnerabilities in network configuration exposed agency systems to attack. These vulnerabilities stemmed from agencies' failure to (1) install and maintain effective perimeter security, such as firewalls and screening routers, (2) implement current software patches, and (3) protect against commonly known methods of attack.

Service Continuity Controls

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. It is also essential that the related controls be understood and supported by management and staff throughout the organization. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing.

To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. Agencies should then take steps to prevent and minimize potential damage and interruption. These steps include routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage;

installing environmental controls, such as fire suppression systems or backup power supplies; arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and ensuring that staff and other users of the system understand their responsibilities in case of emergencies. Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. The plan itself should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location[18] and travel and lodging for necessary personnel, off-site storage location for backup files, and procedures for restoring critical applications and their order in the restoration process. In testing the plan, it is most useful to simulate a disaster situation that tests overall service continuity, including whether the alternative data processing site functions as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Such testing not only helps managers identify weaknesses, it also assesses how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred.

Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. Federal agencies depend not only on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and

[18]Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors, such as making arrangements with suppliers of computer hardware and telecommunications services as well as with suppliers of business forms and other office supplies.

data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency. As we reported in September 2000 on the lessons learned from this challenge, developing these plans was one of a number of management practices that, if continued, could improve federal agencies' overall information technology management, particularly in areas such as critical infrastructure protection and security.[19]

The September 11 tragedies demonstrated just how unexpected and disastrous events can be and how absolutely essential it is for the government to be able to continue critical operations and services during emergency situations. In the aftermath of these events, news reports indicate that business continuity and contingency planning has been a critical factor in restoring operations for New York's financial district, with some specifically attributing companies' preparedness to the contingency planning efforts begun for the Year 2000 challenge. In particular, the Year 2000 challenge increased management attention on continuity and risk management. It also gave companies a chance to rehearse a disaster beforehand.

However, while the Year 2000 challenge increased the focus on business continuity and contingency planning, our analysis of reports since July 1999 showed that most federal agencies covered by our review had service continuity control weaknesses. Examples of common weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.
- Disaster recovery plans were not fully tested to identify their weaknesses. For example, agencies had not performed periodic walkthroughs or unannounced tests of the disaster recovery plan—tests that provide a scenario more likely to be encountered in the event of an actual disaster.

Our more recent work also confirms that service continuity weaknesses continue to exist. For example, in July, we reported that while the Department of the Interior's National Business Center had conducted comprehensive tests of its disaster recovery plan for its computer center,

[19] *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges* (GAO/AIMD-00-290, September 12, 2000).

improvements were still needed in some areas of its overall plan.[20] One of the weaknesses was that the center had not conducted unannounced tests or walkthroughs of its disaster recovery plan. Instead, all tests had been planned with participants fully aware of the disaster recovery test scenario, unlike in an actual disaster, when there is usually little or no warning. In addition, critical backup files for financial and sensitive agency personnel programs, data, and software stored off site were not inventoried. As a result, if a disaster befell the center's main computer facility, there were no assurances that all critical and sensitive system resources would be available to fully restore all key systems.

As another example, in August, we reported that of the seven Department of Commerce (Commerce) bureaus we reviewed,[21] none had developed comprehensive plans to ensure the continuity of service in the event of a service disruption.[22] Specific service continuity weaknesses identified included the following:

- None of the seven bureaus had completed recovery plans for all their sensitive systems.
- Although one bureau had developed two recovery plans, one for its data center and another for its software development installation center, the bureau did not have plans to cover disruptions to the rest of its critical systems, including its local area network.
- Systems at six of the seven bureaus did not have documented backup procedures.
- One bureau stated that it had an agreement with another Commerce bureau to back it up in case of disruptions; however, this agreement had not been documented.
- One bureau stated in its backup strategy that tapes used for system recovery were neither stored off-site nor protected from destruction. For example, backup for its network file servers is kept in a file cabinet in a bureau official's supply room, and backup tapes for a database and web

[20]GAO-01-615 (July 3, 2001).

[21]The seven Commerce bureaus we reviewed were the Bureau of Export Administration, the Economic Development Administration, the Economics and Statistics Administration, the International Trade Administration, the Minority Business Development Agency, the National Telecommunications and Information Administration, and the Office of the Secretary. [For the sake of simplification, we use the term "bureaus" to refer to all seven Commerce organizations, although the Office of the Secretary is not a bureau.] All of these bureaus are based at the Hoover Building in Washington, D.C., and have missions related to or support for trade development, reporting, assistance, regulation, and oversight.

[22]GAO-01-751 (August 13, 2001).

server are kept on the shelf above the server. In case of a destructive event, the backups could be subject to the same damage as the primary files.

- Two bureaus had no backup facilities for key network devices such as firewalls.

Security Program Management Can Be Improved With New Evaluation and Reporting Requirements

Our prior information security reports include many recommendations to individual agencies that address specific weaknesses in the areas I have just described. Agencies have taken steps to address problems, and many have remedial efforts underway. However, these efforts will not be fully effective and lasting unless they are supported by a strong agencywide security management framework.

Establishing such a management framework requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). Our study found that these organizations managed their information security risks through a cycle of risk management activities that included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet these needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

In addition, a strong, centralized focal point can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computing environments.

Implementing this cycle of risk management activities is the key to ensuring that information security risks are adequately considered and addressed on an ongoing, agencywide basis. Included within it are several steps that agencies can take immediately. Specifically, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. Although none of these actions alone will ensure good security, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay.

Due to concerns about the repeated reports of computer security weaknesses at federal agencies, in late 2000, Congress enacted government information security reform legislation as part of the Fiscal Year 2001 National Defense Authorization Act to require agencies to implement the activities I have just described. In addition to requiring security program management improvements, the new provisions require that both management and agency inspectors general annually evaluate agency information security programs. The Office of Management and Budget (OMB) asked agencies to submit the results of their program reviews and the results of their inspector general's independent evaluation by September 10. In accordance with the new law, OMB plans to develop a summary report to the Congress later this year. This summary report, and the subordinate agency reports, should provide a more complete picture of the status of federal information security than has previously been available, thereby providing the Congress and OMB with an improved means of overseeing agency progress and identifying areas needing improvement.

This annual evaluation and reporting process is an important mechanism, previously missing, for holding agencies accountable for implementing effective security and managing the problem from a governmentwide perspective. We are currently reviewing agency implementation of the new provisions.

Critical Infrastructure Protection Efforts Supplement Traditional Information Security

Beyond the risks of computer-based attacks on critical federal operations, the federal government has begun to address the risks of computer-based attacks on our nation's computer-dependent critical infrastructures, such as electric power distribution, telecommunications, and transportation systems. Although these efforts pertain to many traditional computer security issues, such as maintaining the integrity, confidentiality, and availability of important computerized operations, they focus primarily on risks of national importance and encompass efforts to ensure the security of privately controlled critical infrastructures.

The history of federal initiatives to address these computer-based risks includes the following.

- In June 1995, a Critical Infrastructure Working Group, led by the Attorney General, was formed to (1) identify critical infrastructures and assess the scope and nature of threats to them, (2) survey existing government mechanisms for addressing these threats, and (3) propose options for a full-time group to consider long-term government responses to threats to critical infrastructures. The working group identified critical infrastructures, characterized threats to them, and recommended creating a commission to investigate such issues.
- In February 1996, the National Defense Authorization Act required the executive branch to provide a report to the Congress on the policies and plans for developing capabilities to defend against computer-based attacks, such as warnings of strategic attacks against the national information infrastructure.[23] Later that year, the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs, began to hold hearings on security in cyberspace. Since then, congressional interest in protecting national infrastructures has remained strong.
- In July 1996, in response to the recommendation of the 1995 working group, the President's Commission on Critical Infrastructure Protection was established to further investigate the nation's vulnerability to both cyber and physical threats.

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

- In October 1997, the President's Commission issued its report,[24] which described the potentially devastating implications of poor information security from a national perspective.

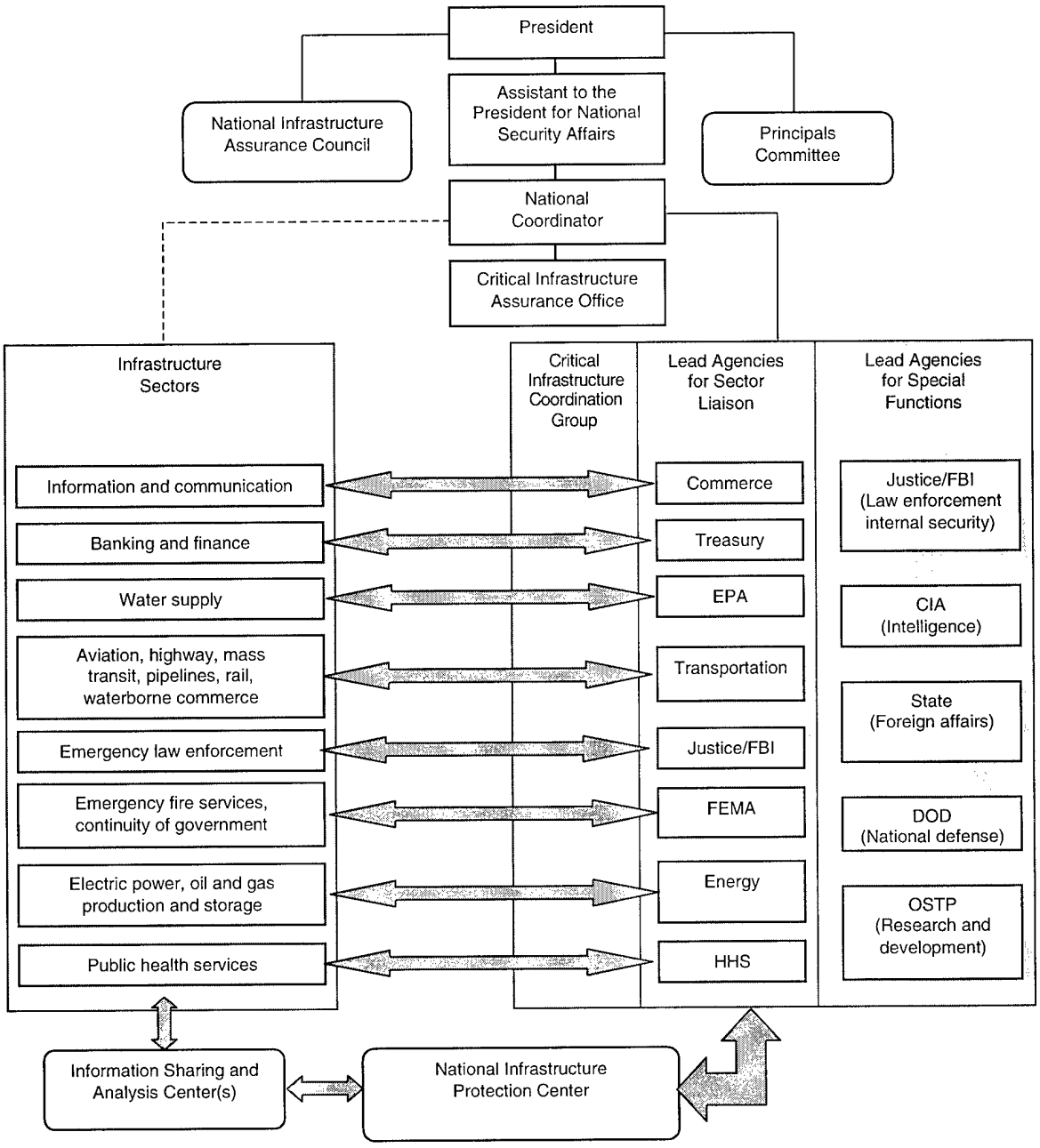
  In response to the commission's report, the President initiated actions to implement a cooperative public/private approach to protecting the nation's critical infrastructures by issuing PDD 63 in May 1998. The directive called for a range of activities to improve federal agency security programs, establish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

  To accomplish its goals, PDD 63 designated the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who reports to the Assistant to the President for National Security Affairs, to oversee the development and implementation of national policy in this area. The directive also established the National Plan Coordination staff, which became the Critical Infrastructure Assurance Office, an interagency office housed in the Department of Commerce responsible for planning infrastructure protection efforts. It further authorized the FBI to expand its National Infrastructure Protection Center (NIPC) and directed the NIPC to gather information on threats and coordinate the federal government's response to incidents affecting infrastructures.

  In addition, the directive designated "lead agencies" to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electric power industry. Similarly, regarding special function areas, DOD is responsible for national defense, and the Department of State is responsible for foreign affairs. To facilitate private-sector participation, PDD 63 encouraged the 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 NIPC. Figure 1 depicts the entities with critical infrastructure protection responsibilities as outlined by PDD 63.

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

Figure 1: Critical Infrastructure Protection Responsibilities as Outlined by PPD 63



Source: The Critical Infrastructure Assurance Office.

Shortly after the initial issuance of PDD 63, we reported on the importance of developing a governmentwide strategy that clearly defines and coordinates the roles of new and existing federal entities to ensure governmentwide cooperation and support for PDD 63.[25] Specifically, we noted that several of PDD 63's provisions appeared to overlap with existing requirements prescribed in the Paperwork Reduction Act; OMB Circular A-130, Appendix III; the Computer Security Act; and the Clinger-Cohen Act. In addition, some of the directive's objectives were similar to objectives being addressed by other federal entities, such as developing a federal incident-handling capability, which was then in the process of being addressed by the National Institute of Standards and Technology and the federal Chief Information Officers Council.[26] At that time, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the Assistant to the President for National Security Affairs ensure such coordination.

In July 2000, we reported that a variety of activities had been undertaken in response to PDD 63, including developing and reviewing individual agency critical infrastructure protection plans, identifying and evaluating information security standards and best practices, and the White House's issuing its *National Plan for Information Systems Protection*[27] as a first major element of a more comprehensive strategy to be developed.[28] At that time, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in PDD 63. On May 9, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and reviewing how the government is organized to deal with

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

[26] The federal incident handling program is now operated by the Federal Computer Incident Response Center at the General Services Administration.

[27] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*, The White House, January 7, 2000.

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

information security issues. Administration officials are currently discussing how the government's strategy for protecting critical computer-dependent infrastructures will relate to the responsibilities of the recently established Office of Homeland Security.

Progress in Implementing PDD 63 Has Been Limited

Last week, as part of our broader report on counterterrorism, we reported that efforts were underway by lead federal agencies, the Critical Infrastructure Assurance Office, and the NIPC to foster cooperative relationships between the federal government and nonfederal sectors. However, efforts to perform substantive analyses of infrastructure vulnerabilities and implementation of remedial actions had been limited.[29]

To assist in establishing relationships with major infrastructure owners and operators, PDD 63 requires lead agencies to assign a high-ranking official, as an agency sector liaison, to lead efforts in cooperation with the sector owners and operators in addressing problems related to critical infrastructure protection and, in particular, in recommending components of a national infrastructure assurance plan. Similarly, the directive required the agency sector liaison officials, after discussions and coordination with entities of their infrastructure sector, to identify infrastructure sector coordinators to represent their sector. In addition, PDD 63 outlined tasks that the lead agencies were to encourage and assist the infrastructure sectors in accomplishing, including developing vulnerability education and outreach programs, establishing ISACs, performing vulnerability assessments of the sectors, and developing related remediation plans.

As of March 2001, each of the eight lead agencies we reviewed had designated sector liaisons, and seven of the eight major infrastructure sectors had identified one or more individuals or groups as sector coordinators for their respective infrastructure sector. Infrastructure sector coordinators had not been selected for the public health services sector because, according to officials at the Department of Health and Human Services, the infrastructure owners and operators had not been fully identified due to the large and diverse communities involved. Also, most infrastructure sectors had planned or held education and outreach events, such as workshops, conferences, and industry meetings to address

[29] *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

broad CIP needs and specific concerns. Further, six ISACs within five infrastructures had been established to gather and share information about vulnerabilities, attempted intrusions, and attacks within their respective infrastructures and to meet specific sector objectives.

However, beyond building partnerships, raising awareness, and improving information sharing, efforts to perform substantive, comprehensive analyses of infrastructure sector vulnerabilities and development of related remedial plans had been limited. While some assessments had been performed for individual sector components, interdependencies within and among the infrastructures had not been fully considered. For example, within the banking and finance sector, while most large institutions had undergone vulnerability assessments, a vulnerability assessment of banking and finance institutions as a group to identify interdependencies and events that could cause a system failure across the infrastructure had not occurred. Such sector-wide assessments had not yet been performed because sector coordinators were still establishing the necessary relationships, identifying critical assets and critical entities, and researching and identifying appropriate methodologies. In addition, some federal officials stated that their agencies did not have the resources to assist in the completion of sector vulnerability assessments.

Factors cited by the private sector as impeding progress in building the necessary government/private-sector partnerships and identifying and addressing vulnerabilities included concerns that (1) organizations potentially could face antitrust violations for sharing information with other industry partners or face potential liabilities for information shared in good faith, (2) sensitive information may be disclosed under the Freedom of Information Act, (3) an inadvertent release of confidential business information, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, and hurt competitiveness, (4) some senior executives were not fully aware of the importance of their assets to the national and economic security of the nation, and (5) organizations capable of coordinating actions across large and complex infrastructures did not exist.

However, other efforts have supplemented lead agency efforts. For example, in December 1999, the Critical Infrastructure Assurance Office helped establish the Partnership for Critical Infrastructure Security as a forum of private-sector member companies for raising awareness and understanding of cross-industry critical infrastructure issues and as a catalyst for action among the owners and operators of the critical infrastructures. As of March 2001, the Partnership had 51 members from various infrastructure sectors. It also had created working groups to address interdependency vulnerability assessment; information sharing,

awareness, and education; legislation and public policy objectives; research and development and workforce development; and organization issues/public private cooperation. Further, the Critical Infrastructure Assurance Office has worked with the audit community to produce and distribute a guide for corporate boards on managing information security risks and coordinated or sponsored a series of conferences to raise awareness—including conferences for the legal community to advance the understanding of legal issues associated with information security.

In addition, the NIPC, which is responsible for analysis, warning, and response related to cyber incidents, had made some progress in establishing cooperative relationships with the private sector. Specifically, in April 2001,[30] we reported that the NIPC had worked to build information-sharing relationships with the private sector through the adoption and expansion of the InfraGard Program, which started in 1996, to provide a secure mechanism for two-way information sharing about intrusion, incidents, and system vulnerabilities. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members included representatives from private industry, other government agencies, state and local law enforcement, and the academic community.

Further, PDD 63 called for a plan to expand international cooperation on critical infrastructure protection and designated the Department of State as the lead agency in this area. According to Department of State officials and the *President's Status Report on CIP*, an international strategy is being implemented that coordinates CIP outreach to other governments and international intergovernmental organizations and promotes CIP awareness, vigilance in security standards and practices, and law enforcement cooperation. As part of this strategy, the Department had organized meetings with key allies to discuss common issues related to infrastructure protection and developed a United Nations Resolution on cybercrime, which passed unanimously in the United Nations General Assembly. In addition, Department of Justice officials were negotiating a Council of Europe convention intended to facilitate international law enforcement issues related to computer crime and, as of March 2001, this treaty still was being negotiated. The Department of Justice also chairs the G-8 High Tech Crime Subgroup that is focused on enhancing law enforcement's abilities to prevent, investigate, and prosecute high-technology crime.[31] Further, Commerce officials had participated in

[30]*Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

[31]Eight major industrialized countries comprise the G-8, which includes Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

meetings with representatives from other countries to discuss and negotiate CIP issues, including the Council of Europe treaty.

In addition to requiring federal departments and agencies to work with the private sector, PDD 63 required them to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by May 2000, and (2) develop procedures and conduct vulnerability assessments. In response, federal agencies have taken initial steps to develop critical infrastructure protection plans, but, as discussed earlier, independent audits continue to identify persistent, significant information security weaknesses that place federal operations at high risk of tampering and disruption.

A March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in agencies' implementation of PDD 63 based on reviews conducted by agency inspectors general.[32] Specifically,

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

The PCIE/ECIE report concluded that the federal government could improve its PDD 63 planning and assessment activities and questioned the federal government's ability to protect the nation's critical infrastructures from intentional destructive acts by May 2003, as required in PDD 63.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective inspectors general reviews.[33] For example, while five agencies had or were in the process of updating their plans, three were not revising their plans to address reported deficiencies. In addition, while most of the agencies we reviewed had identified critical assets, many had not completed related vulnerability assessments. Further, most of the eight agencies we reviewed had not taken the additional steps to identify

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

[33]GAO-01-822 (September 20, 2001).

interdependencies and, as a result, some agency officials said that they were not sure which of their assets were critical from a national perspective and, therefore, subject to PDD 63. Identifying interdependencies is important so that infrastructure owners can determine when disruption in one infrastructure may result in damage to other infrastructures.

We identified several factors that had impeded federal agency efforts to comply with this aspect of PDD 63. First, no clear definitions had been developed to guide development and implementation of agency plans and measure performance. For example, PDD 63 established December 2000 as the deadline for achieving an initial operating capability and May 2003 for achieving full operational capability of key functions. However, the specific capabilities to be achieved at each milestone had not been defined. The PCIE/ECIE report noted that agencies had used various interpretations of initial operating capability and stated that, without a definition, there is no consistent measure of progress toward achieving full security preparedness. In addition, several agency officials said that funding and staffing constraints contributed to their delays in implementing PDD 63 requirements. Further, the availability of adequate technical expertise to provide information security has been a continuing concern to agencies.

Progress in the NIPC Has Been Mixed

A key element of the strategy outlined in PPD 63 was the establishment of the NIPC 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 the 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.

In April, we reported on the NIPC's progress in developing national capabilities for analyzing threat and vulnerability data and issuing warnings, responding to attacks, and developing information-sharing relationships with government and private-sector entities.[34] Overall, we found that while progress in developing these capabilities was mixed, the

[34]GAO-01-323 (April 25, 2001).

NIPC had initiated a variety of critical infrastructure protection efforts that had laid a foundation for future governmentwide efforts. In addition, the NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical and information-sharing capabilities that PDD 63 asserted are needed to protect the nation's critical infrastructures had not yet been achieved, and the NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

Multiple Factors Have Limited Development of Analysis and Warning Capabilities

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

Since its establishment in 1998, the NIPC has issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. These analyses have included (1) situation reports related to law enforcement investigations, including denial-of-service attacks that affected numerous Internet-based entities, such as eBay and Yahoo, and (2) analytical support of a counterintelligence investigation. In addition, the NIPC has issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

However, the use of strategic analysis to determine the potential broader implications of individual incidents has 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.

Three factors have hindered the NIPC's ability to develop strategic analytical capabilities.

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

- Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because other federal agencies have not provided the originally anticipated number of detailees. For example, at the close of our review in February, 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 the NIPC's 3-year existence. In addition, the NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.

- Third, the 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 in February 2001, only three industry assessments had been partially completed, and none had been provided to the NIPC.

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

However, I want to emphasize a more fundamental impediment in the NIPC's progress. Specifically, evaluating its progress in developing analysis and warning capabilities was difficult because the entities involved in the government's critical infrastructure protection efforts did not share a common interpretation of the NIPC's roles and responsibilities.

Further, 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 has direct authority for setting NIPC priorities and procedures and providing NIPC oversight. In addition, NIPC's own plans for further developing its analytical and warning capabilities were fragmented and incomplete. 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 April 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 development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources, and
- clearly define the role of the NIPC in relation to other government and private-sector entities.

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

NIPC Coordination and Technical Support Have Benefited Investigative and Response Capabilities

PDD 63 directed the NIPC to provide the principal means of facilitating and coordinating the federal government's response to computer-based incidents. In response, the NIPC undertook efforts in two major areas: providing coordination and technical support to FBI investigations and establishing crisis-management capabilities.

First, the NIPC provided valuable coordination and technical support to FBI field offices that established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for NIPC field squads and teams.

While these efforts benefited investigative efforts, FBI and NIPC officials told us that increased computer capacity and data transmission capabilities would improve their ability to promptly analyze the extremely large amounts of data that are associated with some cases. In addition, FBI field offices were not yet providing the NIPC with the comprehensive information that NIPC officials say is needed to facilitate prompt identification and response to cyber incidents. According to field office officials, some information on unusual or suspicious computer-based activity had not been reported because it did not merit opening a case and was deemed to be insignificant. To address this problem, the NIPC established new performance measures related to reporting.

Second, the NIPC developed crisis-management capabilities to support a multiagency response to the most serious incidents from the FBI's Washington, D.C., Strategic Information Operations Center. From 1998 through early 2001, seven crisis-action teams had been activated to address potentially serious incidents and events, such as the Melissa virus in 1999 and the days surrounding the transition to the year 2000, and related procedures have been formalized. In addition, the NIPC coordinated the development of an emergency law enforcement plan to guide the response of federal, state, and local entities.

To help ensure an adequate response to the growing number of computer crimes, we recommended in our April report that the Attorney General, the FBI Director, and the NIPC Director take steps to (1) ensure that the NIPC has access to needed computer and communications resources and (2) monitor the implementation of new performance measures to ensure that field offices fully report information on potential computer crimes to the NIPC.

Progress in Establishing Information-Sharing Relationships Has Been Mixed

Information sharing and coordination among private-sector and government organizations are essential for thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as we testified in July 2000,[35] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

The NIPC's success in this area has been mixed. For example, as discussed earlier, the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, has expanded substantially. However, at the close of our review in February 2001, the NIPC had established a two-way, information-sharing partnership with only one industry ISAC—the electric power industry. The NIPC's dealings with two other ISACs consisted of providing information to them without receiving any in return, and no procedures had been developed for more interactive information sharing. According to NIPC and ISAC officials, the relationships have improved since our report.

Similarly, the NIPC and the FBI made only limited progress in developing a database of the most important components of the nation's critical infrastructures—an effort referred to as the Key Asset Initiative. Although FBI field offices had identified over 5,000 key assets, at the time of our review, the entities that own or control the assets generally had not been involved in identifying them. As a result, the key assets recorded may not be the ones that infrastructure owners consider the most important. Further, the Key Asset Initiative was not being coordinated with other similar federal efforts at DOD and Commerce.

[35] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation* (GAO/T-AIMD-00-268, July 26, 2000). Testimony before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives.

In addition, the NIPC and other government entities had not developed fully productive information-sharing and cooperative relationships. For example, federal agencies have not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's Federal Computer Incident Response Center. Further, NIPC and Defense 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. According to the NIPC director, the relationship between the NIPC and other government entities has improved since our review. In recent testimony, officials from the Federal Computer Incident Response Center and the U.S. Secret Service discussed the collaborative and cooperative relationships between their agencies and the NIPC.

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

To improve information sharing, we recommended in our April report that the Assistant to the President for National Security Affairs

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

We also recommended that the Attorney General task the FBI Director to

- formalize information-sharing relationships between the NIPC and other federal entities and industry sectors and

- ensure that the Key Asset Initiative is integrated with other similar federal activities.

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

Lack of A National Plan Is a Severe Impediment to Progress

Last week we reported that, in addition to the specific impediments previously identified, an underlying deficiency in the implementation of the strategy outlined in PDD 63 is the lack of a national plan that clearly delineates the roles and responsibilities of federal and nonfederal entities and defines interim objectives.[36] We first identified the need for a detailed plan in September 1998, when we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.[37] 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 by achieving three crosscutting infrastructure protection objectives:

- minimize the possibility of significant and successful attacks,
- identify, assess, contain, and quickly recover from an attack, and
- create and build strong foundations, including people, organizations, and laws, for preparing, preventing, detecting and responding to attacks.

[36]GAO-01-822 (September 20, 2001).

[37]GAO/AIMD-98-92 (September 23, 1998).

However, this plan focused largely on federal CIP efforts, saying little about the private-sector role. Subsequently, in July 2000, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.[38]

A more complete plan is needed because, although some progress has been made in implementing PDD 63, questions have surfaced regarding specific roles and responsibilities and the time frames within which objectives are to be met. For example, the PCIE/ECIE reported that several agencies had decided not to implement PDD 63 requirements because they believed that they were exempt from the directive. As a result, these agencies had not prepared CIP plans, identified critical assets, performed related vulnerability assessments, or developed remediation plans. However, according to the Critical Infrastructure Assurance Office, PDD 63 requirements apply to all departments and agencies. Also, as I previously discussed, we found that various officials involved in critical infrastructure protection did not consistently interpret the NIPC's role.

In addition, without clearly defined interim objectives and milestones, the success of efforts to improve federal and nonfederal critical infrastructure protection cannot be measured. The PCIE/ECIE report noted that, as of March 2001, agencies still needed guidance for measuring their progress in identifying critical assets, performing vulnerability assessments, and developing and implementing remedial plans.

A May 2001 White House press statement announced that the administration was reviewing how it was organized to deal with information security issues and that recommendations would be made on how to structure an integrated approach to cyber security and critical infrastructure protection. Specifically, the announcement stated that the White House, federal agencies, and private industry had begun to collaboratively prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and reviewing how the government is organized to deal with information security issues.

However, as of early September, a more complete strategy had not been announced. Accordingly, in our report on combating terrorism, issued last

[38]GAO/T-AIMD-00-268 (July 26, 2000).

week, we made several recommendations to supplement those we had made in the past, including those regarding the NIPC. 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 critical infrastructure protection and related information security activities,
- interim objectives and milestones for achieving critical infrastructure protection goals and a specific action plan for achieving these objectives, including implementation of vulnerability assessments and related remedial plans, and
- performance measures for which entities can be held accountable.

Last week, in response to the September 11 terrorist attacks, the President announced the creation of the Office of Homeland Security to coordinate and strengthen counterterrorism efforts. As yet, it is not clear precisely how efforts to protect against computer-based attacks will be incorporated into this new office's activities. Protecting against computer-based attacks requires vigilance against a broad array of threats that include not only terrorists, but nation states, criminals, and others. Therefore, it is likely that a separate strategy will be needed to ensure that critical computer systems are also protected from other malicious acts and damaging events, such as fraud, espionage, and disruptions stemming from natural disasters. However, it will be essential to link the government's strategy for combating computer-based attacks to the national strategy for combating terrorism.

* * * * *

In conclusion, efforts are underway to mitigate the risks of computer-based attacks on federal information systems and on our national computer-dependent infrastructures. However, recent reports and events indicate that these efforts are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks. The evaluation and reporting requirements of the new Government Information Security Reform provisions should help provide a more complete and accurate picture of federal security weaknesses and a means of measuring progress. In addition, it is important that the government ensure that our nation has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damage to our critical infrastructures. However, developing the needed capabilities will require overcoming many challenges. Meeting these challenges will not be easy

and will require clear central direction and dedicated expertise and resources from multiple federal agencies, as well as support from the private sector.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have at this time. If you should have any questions later about this testimony, please contact me at (202) 512-6253. I can also be reached by e-mail at willemssenj@gao.gov.