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., EST
Tuesday,
November 19, 2002

COMPUTER SECURITY

Progress Made, But Critical Federal Operations and Assets Remain at Risk

Statement of Robert F. Dacey
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

GAO-03-303T

November 2002

COMPUTER SECURITY

Progress Made, But Critical Federal Operations and Assets Remain at Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-303T, a testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives.

Why GAO Did This Study

Protecting the computer systems that support our critical operations and infrastructures has never been more important because of the concern about attacks from individuals and groups with malicious intent, including terrorism. These concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

As with other large organizations, federal agencies 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, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information. At the subcommittee's request, GAO discussed its analysis of recent information security audits and evaluations at 24 major federal departments and agencies.

www.gao.gov/cgi-bin/getrpt?GAO-03-303T.

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

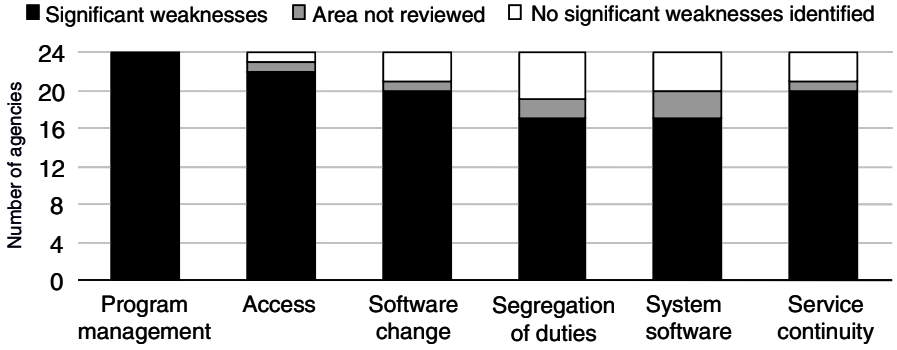
What GAO Found

Although GAO's current analyses of audit and evaluation reports for the 24 major departments and agencies issued from October 2001 to October 2002 indicate some individual agency improvements, overall they continue to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. GAO identified significant weaknesses in each of the 24 agencies in each of the six major areas of general controls. As in 2000 and 2001, weaknesses were most often identified in control areas for security program management and access controls. All 24 agencies had weaknesses in security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented (see figure below for list of major weaknesses).

Implementation of the Government Information Security Reform provisions ("GISRA") is proving to be a significant step in improving federal agencies' information security programs. It has also prompted the administration to take important actions to address information security, such as integrating security into the President's Management Agenda Scorecard. However, GISRA is scheduled to expire on November 29, 2002. GAO believes that continued authorization of such important information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses.

In addition to reauthorizing this legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; providing more specific guidance on the controls agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued October 2001 through October 2002.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our analyses of recent information security audits and evaluations at federal agencies. As with other large organizations, federal agencies 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, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information.

Our analyses considered the results of information security audits and evaluations reported by GAO and inspectors general (IGs) from October 2001 to October 2002 for 24 major federal departments and agencies. In summarizing these results, I will (1) discuss the continuing pervasive weaknesses that led GAO to initially begin reporting information security as a governmentwide high-risk issue in 1997, (2) illustrate the serious risks that these weaknesses pose at selected individual agencies, and (3) describe the major common weaknesses that agencies need to address to improve their information security programs, including agencies' weaknesses in meeting the security requirements of Government Information Security Reform legislation (commonly referred to as "GISRA").[1] Finally, I will discuss some positive actions taken or planned by the administration to improve federal information security, as well as the additional steps needed to develop a comprehensive governmentwide strategy for improvement.

We performed our analyses from September 2002 to November 2002 in accordance with generally accepted government auditing standards.

Results in Brief

Protecting the computer systems that support our nation's critical operations and infrastructures has never been more important. Telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. Yet with this dependency comes an increasing concern about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence

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

gathering, and acts of war. Such concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

Although our current analyses of audit and evaluation reports for the 24 major departments and agencies indicate some individual agency improvements, overall they continue to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, resources, such as federal payments and collections, could be lost or stolen; sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime; and critical operations, such as those supporting national defense and emergency services, could be disrupted.

We identified significant weaknesses in each of the 24 agencies covered by our review and in each of the following six major areas of general controls, that is, 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 areas are security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; access controls, which ensure that only authorized individuals can read, alter, or delete data; software development and change controls, which ensure that only authorized software programs are implemented; segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; system software controls, which protect sensitive programs that support multiple applications from tampering and misuse; and service continuity, which ensures that computer-dependent operations experience no significant disruptions. As in past years' analyses, we identified weaknesses most often for security program management and access controls.

Implementation of GISRA is proving to be a significant step in improving federal agencies' information security programs. It has also prompted the administration to take important actions to address information security, such as plans to integrate security into the President's Management Agenda Scorecard. Although legislation that would reauthorize GISRA is currently being considered, GISRA is scheduled to expire in less than 2 weeks. We believe that continued authorization of such important

information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses.

In addition to Congress' reauthorizing information security legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; providing more specific guidance on the controls that agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

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

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and

intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[2] In addition, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

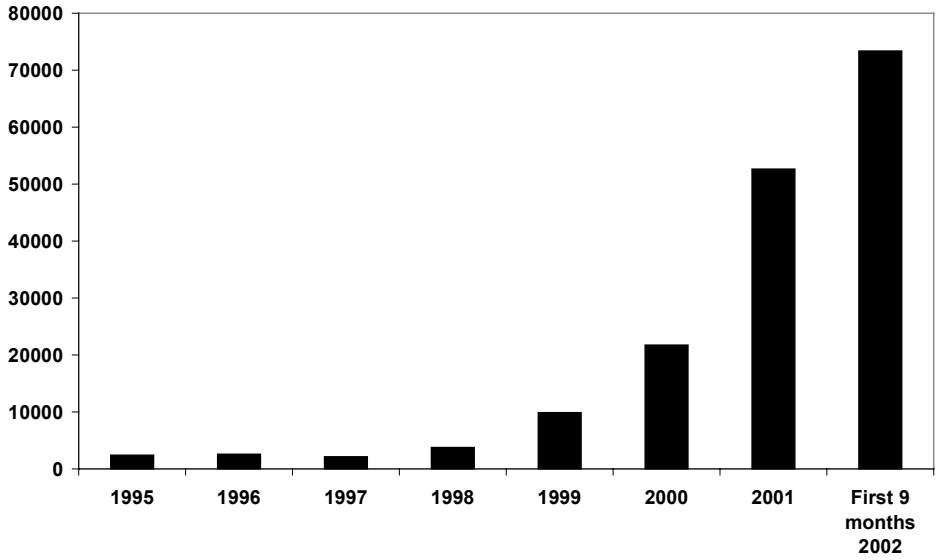
As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A potential hacker can literally download tools from the Internet and "point and click" to start a hack. Experts also agree that there has been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

The April 2002 annual report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had

[2]*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. *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. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

detected computer security breaches. In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 73,359 for just the first 9 months of 2002.[3] And these are only the reported attacks. The Director, CERT® Centers, stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack, or (2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT Coordination Center from 1995 through the first 9 months of 2002.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center from 1995 to the First 9 Months of 2002



Source: Carnegie-Mellon's CERT Coordination Center.

The risks posed by this increasing and evolving threat are demonstrated in reports of actual attacks and disruptions, as well as by continuing government warnings. For example:

[3]CERT® Coordination Center (CERT-CC) 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.

- Just last week, news reports indicated that a British computer administrator was indicted on charges that he broke into 92 U.S. computer networks in 14 states belonging to the Pentagon, private companies, and the National Aeronautics and Space Administration during the past year, causing some $900,000 in damage to computers. It also reported that, according to a Justice Department official, these attacks were one of the biggest hacks ever against the U.S. military. This official also said that the attacker used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks looking for ones that might suffer from flaws in Microsoft Corporation's Windows NT operating system software.

- The FBI's National Infrastructure Protection Center (NIPC) reported that on October 21, 2002, all of the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive "distributed denial of service" attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages. However, according to the media reports, a longer, more extensive attack could have seriously damaged worldwide electronic communications.

- In September 2002, NIPC issued a warning of cyber attacks against the International Monetary Fund and World Bank meetings to be held during the week of September 23.[4] The warning stated that, in addition to physical protestors, cyber groups might view the meetings as a platform to display their hacking talent or to propagate a specific message. Cyber protestors, referred to as "hacktivists," can engage in Web page defacements, denial-of-service attacks, and misinformation campaigns, among other attacks.

- In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[5] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to

[4]National Infrastructure Protection Center, Assessment 02-002:*Hacktivism in Connection with Protest Events of September 2002* (Washington, D.C.: Sept. 23, 2002)

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

manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. Consistent with this threat, NIPC also released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[6]

- In August 2001, we reported to this subcommittee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations.[7] Then in September 2001, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus that allowed it to spread widely in a short amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage.

Since the September 11, 2001, attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups such as al Qaeda have used the Internet to launch a known attack on the United States infrastructure, information on computerized water systems was discovered on computers found in al Qaeda camps in Afghanistan. Also, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[8] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature will become an increasingly viable option for terrorists as they and

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

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

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

other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, Congress enacted GISRA, which became effective November 29, 2000, and is in effect for 2 years. GISRA supplements information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by the Office of Management and Budget (OMB)[9] and the National Institute of Standards and Technology (NIST),[10] as well as audit and best practice guidance issued by GAO.[11] Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establishes new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

GISRA assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and the IGs. OMB is responsible for establishing and overseeing policies, standards and guidelines for information security. This includes the authority to approve agency information security programs, but delegates OMB's responsibilities regarding national security systems to national security agencies. OMB is also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. GISRA does not specify a date for this report, and OMB released its fiscal year 2001 report in February 2002.

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

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

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

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

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

In addition to the responsibilities listed above, GISRA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non-national-security systems are to be performed by the agency IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. For the evaluation of national security systems, special provisions include designation of evaluators by national security agencies, restricted reporting of evaluation results, and an audit of the independent evaluation performed by the IG or an independent evaluator. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

Finally, GISRA also assigns additional responsibilities for information security policies, standards, guidance, training, and other functions to other agencies. These agencies are NIST, the Department of Defense, the Intelligence Community, the Attorney General, the General Services Administration, and the Office of Personnel Management.

Weaknesses in Federal Systems Remain Pervasive

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[12] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in 1998, 2000, and 2001, we analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[13] 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.[14]

Our most recent analyses, of reports issued from October 2001 through October 2002, continue to show significant weaknesses in federal computer systems that put critical operations and assets at risk. Weaknesses continued to be reported in each of the 24 agencies included in our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems

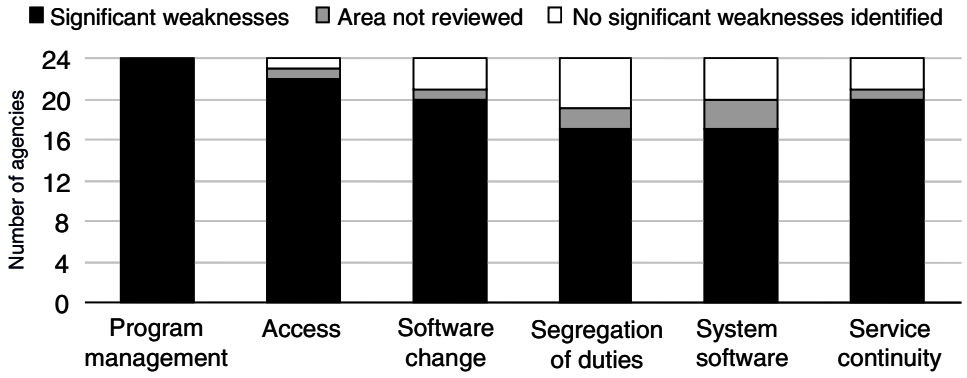
[12]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*. GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

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

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

controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 2 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 2: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued October 2001 through October 2002.

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

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

- For *access controls*, we found weaknesses for 22 of 24 agencies (92 percent) in 2002 (no significant weaknesses were found for one agency, and access controls were not reviewed for another). This compares to access control weaknesses found in all 24 agencies for both 2001 and 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or

sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In addition, it should also be emphasized that our current analyses showed service-continuity-related weaknesses at 20 of the 24 agencies (83 percent) with no significant weaknesses found for 3 agencies (service continuity controls were not reviewed for another). This compares to 19 agencies with service continuity weaknesses found in 2001 and 20 agencies found in 2000. Service continuity controls are important in that they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission. Further, such controls are particularly important in the wake of the terrorist attacks of September 11, 2001.

Our current analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

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

for nonfinancial systems has also increased as agencies and their IGs review and evaluate their information security programs as required by GISRA.

As previously reported, information security weaknesses are also indicated by limited agency progress in implementing Presidential Decision Directive (PDD) 63 to protect our nation's critical infrastructures from computer-based attacks. Issued in May 1998, PDD 63 established critical infrastructure protection as a national goal and called for a range of activities to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious attacks. Critical infrastructure protection involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety. 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.

Last year, the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) reported on the federal government's compliance with PDD 63. It concluded that the federal government could improve its planning and assessment activities for cyber-based critical infrastructures. Specifically, the council stated that (1) many agency infrastructure plans were incomplete; (2) most agencies had not identified their mission-critical infrastructure assets; and (3) few agencies had completed vulnerability assessments of mission-critical assets or developed remediation plans. Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems.[15] For example, although most of the agencies we reviewed had identified critical assets, many had not completed related vulnerability assessments. Further, most of the agencies we reviewed had not taken the additional steps to identify 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

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

determine when disruption in one infrastructure could result in damage to other infrastructures.

In addition, our review of fiscal year 2001 GISRA implementation showed that of the 24 large agencies we reviewed, 15 had not implemented an effective methodology, such as Project Matrix™ reviews, to identify their critical assets.[16] The Department of Commerce's Critical Infrastructure Assurance Office (CIAO) established Project Matrix™ to provide a standard methodology for identifying all assets, nodes, networks, and associated infrastructure dependencies and interdependencies required for the federal government to fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people. In addition, in an effort to more clearly identify and prioritize the security needs for government assets, in February 2002 OMB reported that it planned to direct all large agencies to undertake a Project Matrix™ review to identify critical infrastructure assets and their interdependencies with other agencies and the private sector. As of July 2002, CIAO reported that most agencies had not completed Project Matrix™ step 1 to identify their critical assets, and few had even begun step 2 to identify other federal government assets, systems, and networks on which their critical assets depend to operate.

Substantial Risks Persist for Federal Operations, Assets, and Confidentiality

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

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

- resources, such as federal payments and collections, could be lost or stolen;

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

- computer resources could be used for unauthorized purposes or to launch attacks on others;

- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of crime;

- critical operations, such as those supporting national defense and emergency services, could be disrupted;

- data could be modified or destroyed for purposes of fraud or disruption; or

- agency missions could be undermined by embarrassing incidents that result in diminished confidence in the agencies' ability to conduct operations and fulfill their fiduciary responsibilities.

Recent audits show that while agencies have made some progress, weaknesses continue to be a problem and that critical federal operations and assets remain at risk.

- In February 2002, we reported that the Internal Revenue Service (IRS) corrected or mitigated many of the computer security weaknesses identified in our previous reports, but much remains to be done to resolve the significant control weaknesses that continue to exist within IRS's computing environment and to be able to promptly address new security threats and risks as they emerge.[17] Weaknesses found, such as not always adequately restricting electronic access within its computer networks and to its systems, can impair the agency's ability to perform vital functions and increase the risk that unauthorized individuals could gain access to critical hardware and software and intentionally or inadvertently view, alter, or delete sensitive data or computer programs. Also, such weaknesses increase the risk that individuals could obtain personal taxpayer information and use it to commit financial crimes in taxpayers' names (identity fraud), such as establishing credit and incurring debt.

- In April 2002, the IG for the Department of Justice reported serious deficiencies in controls for five sensitive-but-unclassified systems that

[17]U.S. General Accounting Office, *Financial Audit: IRS's Fiscal Year 2001 and 2000 Financial Statements*, GAO-02-414 (Washington, D.C.: Feb. 27, 2002).

support critical departmental functions, such as tracking prisoners; collecting, processing, and disseminating unclassified intelligence information; and providing secure information technology facilities, computing platforms, and support services.[18] The most significant of these deficiencies concerned the technical controls that help prevent unauthorized access to system resources. Because of the repetitive nature of the security deficiencies and concerns identified, the IG recommended that a central office responsible for system security be established to identify trends and enforce uniform standards. The IG also included other specific recommendations intended to improve departmentwide computer security for both classified and sensitive-but-unclassified systems. In addition to this report, in March 2002, the Commission for Review of FBI Security Programs reported that the FBI's information systems security controls were inadequate.

- In June 2002, we reported that the U.S. Army Corps of Engineers had made substantial progress in improving computer controls at each of its data processing centers and other Corps sites since our 1999 review, but that continuing and numerous newly identified control vulnerabilities continued to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data.[19] These vulnerabilities warranted management's attention to decrease the risk of inappropriate disclosure and modification of data and programs, misuse of or damage to computer resources, or disruption of critical operations. These vulnerabilities also increased risks to other DOD networks and systems to which the Corps' network is linked.

- In our September 2002 testimony, we reported that the Department of Veterans Affairs (VA) had taken important steps to strengthen its computer security management program, including increasing security training; providing a more solid foundation for detecting, reporting, and responding to security incidents; and reducing the risk of unauthorized access through external connections to its critical systems. Nonetheless, the department had not yet fully implemented a comprehensive computer security management program that included a process for routinely

[18]Office of the Inspector General, U.S. Department of Justice, *Independent Evaluation Pursuant to the Government Information Security Reform Act – Fiscal Year 2001 – Sensitive But Unclassified Systems*, Report Number 02-18, April 2002.

[19]U.S. General Accounting Office, *Information Security: Corps of Engineers Making Improvements, But Weaknesses Continue*, GAO-02-589 (Washington, D.C.: June 10, 2002).

monitoring and evaluating the effectiveness of security policies and controls and addressing identified vulnerabilities. Further, VA's offices were self-reporting computer security weaknesses, and the department lacked an independent component to ensure the accuracy of reporting and validating corrective actions taken.

- Department of Commerce officials have shown a commitment to correcting vulnerabilities identified in our August 2001 report.[20] They indicate that they have developed and implemented an action plan for strengthening access controls for the department's sensitive systems, published policy on comprehensive recovery plans which applies to all Commerce operating units to help ensure continuity of operations, and began the process of establishing a department-wide incident handling capability with formal procedures for preparing for, detecting, responding to, and reporting incidents. While neither the department's inspector general nor GAO has validated these corrective actions, these responses show that the agency is attempting to quickly address identified weaknesses.

Similar Control Weaknesses Continue Across Agencies

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 effect on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. Likewise, similarities exist in the corrective actions agencies 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 analyses.

Security Program Management Controls

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 problem has been detected or an audit finding reported.

[20]U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*, GAO-01-751 (Washington, D.C.: Aug. 13, 2001).

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. All the agencies for which this aspect of security was reviewed had deficiencies. 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, or
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Establishing a strong security management program 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 the 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 these risk management activities are several steps that agencies can take immediately. Specifically, agencies 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, these are steps that can be made without delay.

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 that we have commonly identified include the following:

- Accounts and passwords for individuals no longer associated with an agency are not deleted or disabled or are not adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, in some cases, former employees and contractors could still (and in many cases did) read, modify, copy, or delete data; and even after long periods of inactivity, many users' accounts had not been deactivated.

- Users are not required to periodically change their passwords.

- Managers do not precisely identify and document access needs for individual users or groups of users. Instead, they provide overly broad access privileges to very large groups of users. For example, some operating system files were not protected from unauthorized access, permitting general users full access to these files. This would enable users to obtain passwords and system administration privileges, allowing a person to log in as someone else and use that access to read files, destroy or alter data, and initiate transactions.

- Use of default, easily guessed, and unencrypted passwords significantly increases the risk of unauthorized access. We are often able to guess many passwords on the basis of our knowledge of commonly used passwords and to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.

- Vendors' default passwords or off-the-shelf parameters are used that do not meet the password requirements specific to the agency.

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. In almost every test, our auditors have been successful 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. Much of the activity associated with our intrusion

testing had 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 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.

Examples of weaknesses in this area include the following:

- Testing procedures are undisciplined and do not ensure that implemented software operates as intended. For example, fully developed procedures may not exist for controlling changes over software that would prevent unauthorized programs or modifications to an existing program to be implemented. Also, documentation is not always maintained to show that program changes have been tested, independently reviewed, and approved for implementation.

- Implementation procedures do not ensure that only authorized software is used. In particular, lack of adequate follow-up and documentation procedures for making emergency software changes increases the risk of software errors, which could cause system failures and/or data loss.

- Agencies' policies and procedures frequently do not address the maintenance and protection of program libraries. For example, the management software was not used to produce audit trails of program changes, maintain program version numbers, record and report program

changes, maintain date information for production modules, and maintain copies of previous versions and control concurrent updates.

Segregation of Duties Controls

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, a 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. Common problems involve computer programmers and operators who are authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. An example of this would be a single individual authorized to independently develop, test, review, and approve software changes for implementation.

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 security controls over the operating system 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 previously discussed. 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. A common type of problem reported is insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. Further, pervasive vulnerabilities in network configuration expose agency systems to attack. These vulnerabilities stem 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

The terrorist attacks that began on September 11, 2001, have redefined the disasters that must be considered in identifying and implementing service continuity controls to 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, on the basis of 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 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[21] 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.

Contingency planning should also 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 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

[21]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.

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.[22] For example, in the aftermath of the attacks of September 11, 2001, news reports indicate that business continuity and contingency planning was 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.

Despite this increased focus on business continuity and contingency planning, our analyses show that most federal agencies currently have service continuity control weaknesses. Examples of common agency weaknesses include 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.

GISRA Spurs Agency Actions, But Highlights Weaknesses

As we reported in March 2002, first-year GISRA implementation demonstrated that the new law provides a significant step in improving federal agencies information security programs.[23] To implement GISRA requirements and comply with OMB guidance, agencies reviewed their information security programs, reported the results of these reviews and their IGs' independent evaluations to OMB, and developed plans to correct identified weaknesses. In addition, GISRA implementation has also resulted in important actions by the administration, which if properly implemented, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is

[22]U.S. General Accounting Office, *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges*, GAO/AIMD-00-290 (Washington, D.C.: Sept. 12, 2000).

[23]GAO-02-470T.

incorporated into and funded as part of each investment. Administration actions and plans also include

- directing all large agencies to undertake a review to identify and prioritize critical assets within the agencies and their interrelationships with other agencies and the private sector, as well as a cross-government review to ensure that all critical government processes and assets have been identified;
- integrating security into the President's Management Agenda Scorecard;
- developing workable measures of performance;
- developing e-training on mandatory topics, including security; and
- exploring methods to disseminate vulnerability patches to agencies more effectively.

Other actions include additional security guidance by OMB and NIST. For example, OMB has provided the agencies with specific performance measures for agency officials who are accountable for information and information technology security and required the agencies to report actual performance for these measures in their fiscal year 2002 GISRA reports. Further, NIST-developed guidance includes a Security Self-Assessment Guide and supporting tools to help agencies perform self-assessments of their information security programs.[24] This guide accompanies NIST's Security Assessment Framework methodology, which agency officials can use to determine the current status of their security programs.[25] The guide itself uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. Many agencies used a draft version of the self-assessment guide for their fiscal year 2001 GISRA program reviews, and with issuance of a final version in November 2001, OMB now requires that the guide be used for fiscal year 2002 reviews. Also, NIST developed a tool to automate completion of the

[24]National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001.

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

guide's questionnaire that can be found at its Computer Security Resource Center web site: http://csrc.nist.gov/asset/.

In addition to these actions, the actual results of GISRA reviews and evaluations have helped to further highlight where agencies have not established information security programs consistent with GISRA requirements and where significant weaknesses exist. In its fiscal year 2001 report to the Congress on GISRA, OMB noted that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security.[26] In particular, the report highlights six common security weaknesses: (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

Our analyses of the results of agencies' fiscal year 2001 GISRA reviews and evaluations also showed that agencies are making progress in addressing information security, but that none of the agencies had fully implemented the information security requirements of GISRA and all continue to have significant weaknesses. In particular, our review of 24 of the largest federal agencies showed that agencies had not fully implemented requirements to

- conduct risk assessments for all their systems;
- establish information security policies and procedures that are commensurate with risk and that comprehensively address the other reform provisions;
- provide adequate computer security training to their employees, including contractor staff;

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

- test and evaluate controls as part of their management assessments;
- implement documented incident handling procedures agencywide;
- identify and prioritize their critical operations and assets and determine the priority for restoring these assets should a disruption in critical operations occur; or
- have a process to ensure the security of services provided by a contractor or another agency.

According to OMB's July 2002 guidance, agencies and their IGs were required to submit the results of their fiscal year 2002 GISRA reviews and evaluations to OMB by September 16, 2002, and to submit corrective action plans by October 1. Our most recent analyses of audit reports and evaluations to identify significant information security weaknesses considered the results of the IGs' fiscal year 2002 GISRA independent evaluations. In addition, in response to a request by this subcommittee, we are currently evaluating the results of agencies' second-year GISRA implementation; our evaluation is to include an analysis of agencies' corrective action plans and their progress in correcting identified weaknesses.

At this time, however, GISRA is still scheduled to expire on November 29, 2002. And although several bills would address GISRA reauthorization, none have yet been enacted. We believe that continued authorization of such important information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses. Further, this authorization would reinforce the federal government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

Improvement Efforts Are Underway, But Challenges Remain

Information security improvement efforts have been undertaken in the past few years both at an agency and governmentwide level. These efforts include the agency, IG, and OMB actions to implement GISRA information security requirements and correct identified information security weaknesses. In addition, in October 2001, President Bush signed executive

orders creating the Office of Homeland Security and establishing the President's Critical Infrastructure Protection Board.[27] Chaired by the Special Advisor to the President for Cyberspace Security, the board is to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures and recommend policies and coordinating programs for protecting information systems related to critical infrastructure protection. In addition, the board is intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure.

In July 2002, the President also issued the National Strategy For Homeland Security to "mobilize and organize our nation to secure the United States homeland from terrorist attacks."[28] According to the strategy, the primary objectives of homeland security in order of priority are to (1) prevent terrorist attacks within the United States, (2) reduce America's vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur. This strategy also calls for the Office of Homeland Security and the President's Critical Infrastructure Protection Board to complete cyber and physical infrastructure protection plans, which would serve as the baseline for developing a comprehensive national infrastructure protection plan. While the national strategy does not indicate a date when the comprehensive plan is to be completed, in September 2002, the board released a comment draft of a National Strategy to Secure Cyberspace.[29] Defined as a strategy of steps the United States will take to secure the information technology networks necessary for the nation's economy, defense, and critical services to operate, the strategy is divided into five audience levels ranging from home users and small businesses to discussion of global issues. Level 3 describes the issues and challenges of, and makes recommendations for, critical sectors, including the federal government, state and local government, higher education, and the private sector.

[27]"Establishing the Office of Homeland Security and the Homeland Security Council," Executive Order 13228, October 8, 2001 and "Critical Infrastructure Protection in the Information Age," Executive Order 13231, October 16, 2001.

[28]Office of Homeland Security, the White House, *National Strategy for Homeland Security*, July 2002.

[29]The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace—For Comment Draft*, September 2002.

These actions are laudable. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces the challenge of ensuring that risks from cyber threats are appropriately addressed. Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement.

We believe that the following seven steps should be taken as part of a comprehensive strategy for improvement.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security. This strategy should also consider other organizations with information security responsibilities, including OMB, which oversees and coordinates federal agency security, and interagency bodies like the CIO Council, which are attempting to coordinate agency initiatives. It should also describe how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[30] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Implementing such standards for federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of

[30]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category. At this time, NIST plans to publish a special publication in Spring 2003 that establishes a set of standardized, minimum security controls for information technology systems addressing low, moderate, and high levels of concern for confidentiality, integrity, and availability.

Third, ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA, would allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and monitoring process established through GISRA is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.

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

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

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. In our review of first-year GISRA implementation, we reported that many agencies emphasized the need for adequate funding to implement security requirements, and that security funding varied widely across the agencies. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, additional amounts are likely to be needed to address specific weaknesses and new tasks. At the same time, OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not

using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process. Further, we agree with OMB that much can be done to cost-effectively address common weaknesses, such as security training, across government rather than individually by agency.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. In addition, in its December 2001 third annual report, the Gilmore Commission recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.[31] In this regard, the Congress recently passed the Cyber Security Research and Development Act (H.R. 3394) to provide $903 million over 5 years for cybersecurity research and education programs. This bill, which has been sent to the President for signature, would direct the National Science Foundation to create new cybersecurity research centers, program grants, and fellowships. It would also direct NIST to create new program grants for partnerships between academia and industry.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at daceyr@gao.gov.

[31] *Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Dec. 15, 2001).