GAO

United States General Accounting Office

Testimony

Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives

INFORMATION SECURITY

Further Efforts Needed to Fully Implement Statutory Requirements in DOD

Statement of Robert F. Dacey
Director, Information Security Issues

G A O
Accountability * Integrity * Reliability

GAO-03-1037T

July 24, 2003

INFORMATION SECURITY

Further Efforts Needed to Fully Implement Statutory Requirements in DOD

Why GAO Did This Study

The Department of Defense (DOD) faces many risks in its use of globally networked computer systems to perform operational missions—such as identifying and tracking enemy targets—and daily management functions—such as paying soldiers and managing supplies. Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.

GAO was asked, among other things, to discuss DOD's efforts to protect its information systems and networks from cyber attack, focusing on its reported progress in implementing statutory information security requirements.
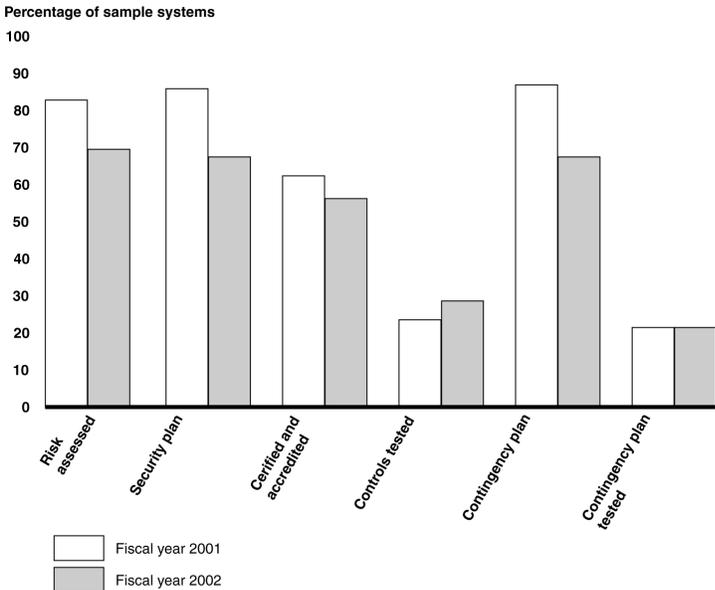
What GAO Found

In its fiscal year 2002 report on efforts to implement information security requirements under Government Information Security Reform law, DOD reported that it has an aggressive information assurance program and highlighted several initiatives to improve it. These initiatives included developing an overall strategy and issuing numerous departmentwide information security policy documents. DOD's reporting highlighted other accomplishments, but acknowledged that a number of challenges remain for the department in implementing both its policies and procedures and statutory information security requirements.

DOD reported several material control weaknesses, which included needing to decrease the time necessary for correcting reported weaknesses and ensuring that computer security policies are enforced and security capabilities are tested regularly. Further, performance data DOD reported for a sample of its systems showed that further efforts are needed to fully implement key information security requirements, such as testing systems' security controls, throughout the department (see figure).

Although DOD has undertaken its Defense-wide Information Assurance Program to promote integrated, comprehensive, and consistent practices across the department and has recently issued both policy guidance and implementation instructions, it does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and ensuring that those policies are consistently practiced throughout DOD.

Reported Results for Selected DOD Information Security Performance Measures

Percentage of sample systems

Fiscal year 2001
Fiscal year 2002

United States General Accounting Office

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the status of efforts by the Department of Defense (DOD) to protect its information systems and networks from cyber attack. DOD's military services and agencies face many risks in their use of globally networked computer systems to perform operational missions, such as identifying and tracking enemy targets, and daily management functions, such as paying soldiers and managing supplies. Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.

Since 1996,[1] we have reported that poor information security in federal agencies is a widespread problem with potentially devastating consequences. Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997— most recently in January 2003.[2] Concerned that significant weaknesses in federal computer systems make them vulnerable to attack, in October 2000 the Congress passed and the President signed into law Government Information Security Reform provisions (commonly known as GISRA)[3] to establish information security program, evaluation, and reporting requirements for federal agencies—requirements that are now permanently authorized and strengthened through the recently enacted Federal Information Security Management Act of 2002 (FISMA).[4]

In my testimony today, I will first provide an overview of the increasing nature of cyber security threats and vulnerabilities and of the continuing pervasive weaknesses across the federal government that led GAO to initially begin reporting information security as a high-risk issue. I will

---

[1]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).

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

[3]*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.

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

then discuss the status of DOD's efforts to ensure the security of its information systems and to implement the statutory information security requirements, focusing on the performance data that DOD reported to the Office of Management and Budget (OMB). Finally, I will discuss some of the challenges for the department in establishing an effective information security management program.

In preparing this testimony, we relied on prior reports and testimony on information security both governmentwide and for DOD. We also analyzed reports prepared by the DOD chief information officer and the DOD inspector general (IG) for fiscal year 2002 GISRA reporting, as well as recent DOD policy and guidance documents related to information security. Further, we analyzed OMB's May 2003 report to the Congress on fiscal year 2002 GISRA implementation.[5] We did not validate the accuracy of the data reported by DOD or OMB. We performed our work in July 2003, 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 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 there have been some individual agency improvements, our most recent analyses of audit and evaluation reports for the 24 major departments and agencies continued to highlight significant information security weaknesses that place a broad array of federal operations and

---

[5]Office of Management and Budget, *FY 2002 Report to Congress on Federal Government Information Security Reform*, May 16, 2003.

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, 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.

In its fiscal year 2002 GISRA report, DOD reported that the department has an aggressive information assurance (IA) posture and highlighted several initiatives to improve its IA program.[6] These initiatives included developing an overall strategy that identifies goals and objectives for the program and issuing numerous information security policy directives, instructions, manuals, and policy memorandums. Further, DOD's GISRA reporting highlighted other accomplishments, such as evaluating security controls for a sample of its networks. However, this reporting also showed that a number of challenges remain for the department in implementing both its policies and procedures and statutory information security requirements, as indicated by the material weaknesses it reported related to its IA capabilities, and its performance data that showed further efforts are needed to implement key requirements. For example, specific deficiencies related to DOD's material weaknesses included the need to decrease the time necessary for correcting reported weaknesses and to ensure that computer security policies are enforced and security capabilities are tested regularly. Also, performance data reported by DOD for a sample of its systems showed that further effort is needed by the department to report on all its systems and to fully implement key information security requirements, such as testing systems' information security controls and their contingency plans.

Our past work has shown that an important challenge agencies face in implementing an effective information security management program is ensuring that they have the appropriate management structures and processes in place to strategically manage information security, as well as to ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security. DOD has

---

[6]IA refers to the range of information security activities and functions needed to protect DOD's information and systems.

undertaken its Defense-wide Information Assurance Program (DIAP) to promote integrated, comprehensive, and consistent IA practices across the department and has recently issued both policy guidance and implementation instructions. However, as indicated by the Defense audit community's assessment of the DOD's fiscal year 2001 GISRA data, DOD does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and ensuring that those policies are consistently practiced throughout the department.

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.

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

Table 1: Threats to Critical Infrastructure Observed by the FBI

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

Source: Federal Bureau of Investigation unless otherwise indicated

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

Government officials remain concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming

aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[7] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology (IT), the likelihood increases that information attacks will threaten vital national interests.

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

---

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

Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center[8] has also risen dramatically from 9,859 in 1999 to 82,094 in 2002 and 76,404 for just the first half of 2003. And these are only the reported attacks. The Director of 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 half of 2003.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center from 1995 through the First Half of 2003

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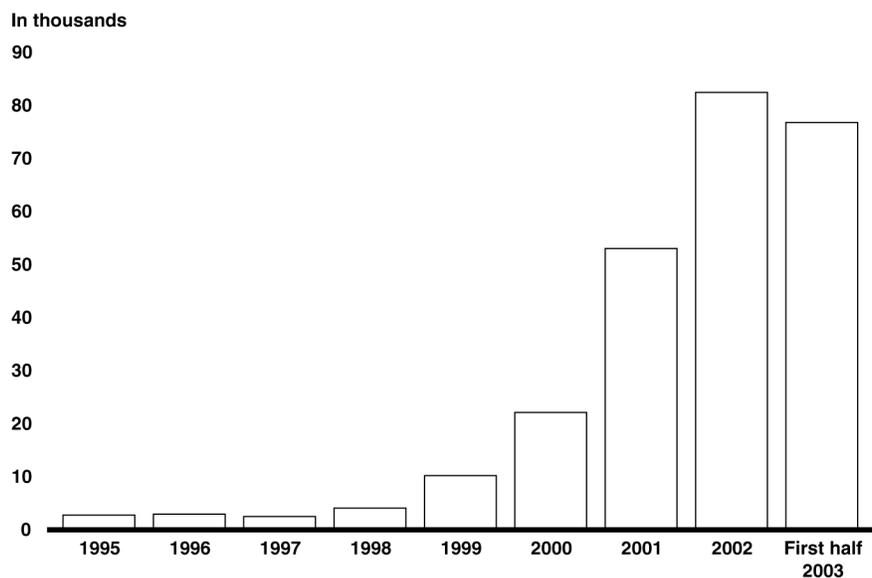
Source: Carnegie-Mellon's CERT® Coordination Center.

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and

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

methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[9] 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.[10] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Since September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized. In his November 2002 congressional testimony, the Director of the CERT Centers at Carnegie-Mellon University noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions.[11] These computer-controlled and network-connected systems

---

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

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

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

are potential targets for individuals bent on causing massive disruption and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers.

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

- On February 11, 2003, the National Infrastructure Protection Center (NIPC) issued an advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq.[12] This advisory noted that during a time of increased international tension, illegal cyber activity often escalates, such as spamming, Web page defacements, and denial-of-service attacks. Further, this activity can originate within another country that is party to the tension, can be state sponsored or encouraged, or can come from domestic organizations or individuals independently. The advisory also stated that attacks may have one of several objectives, including political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers, political activism or disruptive attacks targeting U.S. systems by those opposed to any potential conflict with Iraq, or even criminal activity masquerading or using the current crisis to further personal goals.

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

---

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

malicious payload, attacked a more widespread vulnerability, or targeted a more popular service.

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

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

- In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[13] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. Consistent with this threat, NIPC also released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[14]

---

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

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

- In August 2001, we reported to a subcommittee of the House Government Reform Committee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations.[15] 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.

Significant Weaknesses Persist in Federal Information Security

To better understand the risks facing DOD systems, it is useful to consider the overall status of information security for the federal government. Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. For the past several years, we have analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[16]

As reported in November 2002, our latest analyses of reports issued from October 2001 through October 2002, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[17] Weaknesses continued to be reported in each of the 24 agencies included in our review,[18] and they covered all six major areas of

---

[15]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).

[16]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious* and *Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001); *and Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-03-303T (Washington, D.C.: Nov. 19, 2002).

[17]GAO-03-303T.

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

general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 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

Number of agencies

No significant weaknesses identified

Area not reviewed

Significant weaknesses
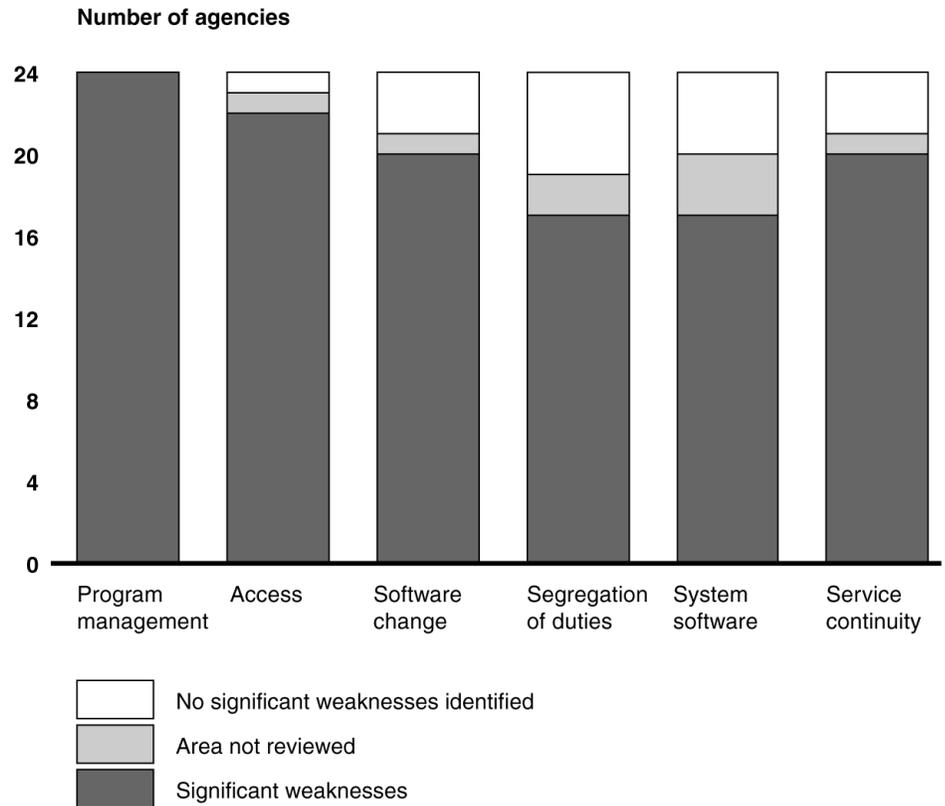
Source: Audit reports issued October 2001 through October 2002.

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

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

For access controls, we found weaknesses for 22 of 24 agencies (92 percent) in 2002 (no significant weaknesses were found for one agency, and access controls were not reviewed for another). This compares to access control weaknesses found in all 24 agencies for both 2000 and 2001. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

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

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

Most of the audits represented in figure 2 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related

operations. However, at agencies whose missions are primarily nonfinancial, such as DOD and the Department of Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. However, in response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems has also increased as agencies and their IGs reviewed and evaluated their information security programs as required by GISRA.

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

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

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

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

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

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

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

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

Congress Consolidates and Strengthens Federal Information Security Requirements

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

Most importantly, however, GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. GISRA assigned specific responsibilities to OMB, agency heads and CIOs, and IGs. OMB was responsible for establishing and overseeing policies, standards, and guidelines for information security. This included the authority to approve agency information security programs, but delegated OMB's responsibilities regarding national security systems to national security agencies. OMB was also required to submit an annual report to the Congress summarizing results of agencies' independent evaluations of their information security programs. OMB released its fiscal year 2001 report in February 2002 and its fiscal year 2002 report in May 2003.

GISRA required each agency, including national security agencies, to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is

---

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

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

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

practiced throughout the life cycle of each agency system. Specifically, this program was to include

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;

- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;

- training on security responsibilities for information security personnel and on security awareness for agency personnel;

- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;

- a process for identifying and remediating any significant deficiencies;

- procedures for detecting, reporting, and responding to security incidents; and

- an annual program review by agency program officials.

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

With GISRA expiring on November 29, 2002, on December 17, 2002, FISMA was enacted as title III of the E-Government Act of 2002 to permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA. Among other things, FISMA also requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of

providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. In addition, FISMA requires each agency to develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is also to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

DOD Highlights Initiatives, But Also Reports Weaknesses

DOD has undertaken several initiatives to improve its information security, including the development of an overall IA strategy and the issuance of information security policy and guidance.[22] However, information that DOD's CIO and IG submitted for fiscal year 2002 GISRA reporting showed that a number of challenges remain for the department in implementing both its policies and procedures and the statutory information security requirements. These challenges are indicated by the material weaknesses DOD reported related to its IA capabilities and its performance data, which showed that further efforts are needed to implement key requirements.

DOD Efforts to Improve Information Security

Overall, the DOD CIO reported in its fiscal year 2002 GISRA report that the department has an aggressive IA posture and highlighted several initiatives to improve its IA program. In particular, DOD has developed an overall IA strategic plan to define the department's goals and objectives and to provide a consistent departmentwide approach to information assurance. Further, according to a DOD official, DOD is aligning its strategic initiatives to objectives in this plan and is developing milestones and performance measures to gauge success.

Specific plan goals include:

---

[22]IA refers to the range of information security activities and functions needed to protect DOD's information and systems.

- protecting information to ensure that all information has a level of trust commensurate with mission needs;

- defending systems and networks to ensure that no access is uncontrolled and that all systems and networks are capable of self-defense; and

- creating an IA-empowered workforce that is trained, highly skilled, knowledgeable, and aware of its role in assuring information.

The plan also identified specific objectives for each goal. For example, to meet the goal of protecting information to ensure that all information has a level of trust commensurate with mission needs, DOD identified objectives including defining data protection requirements, applying protection mechanisms across the enterprise, and developing robust mechanisms that protect information. In addition, DOD has developed a complementary implementation mechanism for IA known as Defense in Depth that uses a multilayered approach with defense mechanisms on successive layers at multiple locations.

Other initiatives highlighted in the DOD CIO's fiscal year 2002 GISRA report included establishing a number of senior-level bodies that discuss, brief, and shape the future of IA efforts—such as the CIO Executive Board and the Military Communications-Electronics Board—and issuing information security policy directives, instructions, manuals, and policy memorandums.

During fiscal year 2003, DOD has continued its efforts to implement IA departmentwide by issuing additional policy and guidance. Specifically, in October 2002, it issued DOD Directive 8500.1 to establish policy and assign responsibility for IA management.[23] Further, in February 2003, DOD issued DOD Instruction 8500.2, which prescribes a framework for implementing the department's IA program and establishes baseline levels of assurance for information systems.[24]

---

[23]Department of Defense Directive Number 8500.1, *Information* Assurance (IA) (Oct. 24, 2002)

[24]Department of Defense Instruction Number 8500.2, *Information Assurance (IA) Implementation* (Feb. 6, 2003).

Material Weaknesses Identified By DOD

DOD reported eight material weaknesses in fiscal year 2002 for which it said it is undertaking aggressive action to improve and expand its IA capabilities. The actions DOD identified to address the eight deficiencies are:

- completing the implementation of the Information Assurance Vulnerability Alert process to all services and agencies;

- ensuring that effective computer security policies and procedures are distributed in a timely manner;

- improving DOD business processes to ensure that all systems are protected;

- decreasing the time necessary for correction of reported weaknesses;

- ensuring that computer security policies are enforced and security capabilities are tested regularly;

- ensuring that training is conducted for all network personnel (this includes awareness training for all personnel to specific network defense training for system and network administrators);

- increasing access security through the use of electronic tokens; and

- increasing security through certificates (for authentication and nonrepudiation).

DOD Reports Show Further Efforts Needed to Implement Key Information Security Requirements

OMB's fiscal year 2002 reporting instructions included new high-level management performance measures that the agencies and IGs were required to use to report on agency officials' performance, such as the number and percentage of systems that have been assessed for risk and that have an up-to-date security plan. In addition, OMB's reporting instructions for fiscal year 2002 stated that agencies were expected to review all systems annually.[25] OMB explained that GISRA requires senior

---

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

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

DOD reported data for most performance measures as required. However, as agreed with OMB, DOD reported these data for only a sample of its systems and networks rather than for all systems. As a result, DOD cannot ensure that these performance measures accurately reflect the information security status of its thousands of systems or that potential weaknesses for all systems have been identified for correction. Further, reporting on only a sample of systems limited the usefulness of OMB's analysis of the governmentwide status of IT security reported in its fiscal year 2002 report to the Congress, which considered data for only DOD's sample of systems in measuring the overall progress by 24 large agencies.

DOD indicated in its report that because of its size and complexity, the collection of specific metrics required sizable lead time to allow for the collection and approval process by each military service and agency. For this reason, DOD focused its fiscal year 2002 GISRA efforts on (1) a sample of 366 of its networks (241 unclassified and 125 classified) and (2) a sample of 155 systems that were selected from the sample of systems used for DOD's fiscal year 2001 GISRA review. Although DOD reported performance measure data for both the sample of networks and the sample of systems, OMB's provided comparative results in its report to Congress primarily for the sample of 155 systems. However, as discussed later in this statement, DOD did report that 96 percent of its sample of networks was certified and accredited.

OMB's fiscal year 2002 GISRA report to the Congress summarized both agency and overall results for certain key measures for 24 large federal agencies. Subject to the limitation of DOD's data, figure 3 summarizes DOD results for six of these measures for the 155 systems and shows that most of these measures actually decreased from fiscal year 2001 to fiscal year 2002. DOD attributed the decreases to inaccuracies in the fiscal year 2001 data. Discussion of these and other measures follow figure 3 and include a comparison of DOD results to results for other agencies as

presented in our recent testimonies before a subcommittee of the House Government Reform Committee.[26]

Figure 3: Reported Results for Selected DOD Information Security Performance Measures
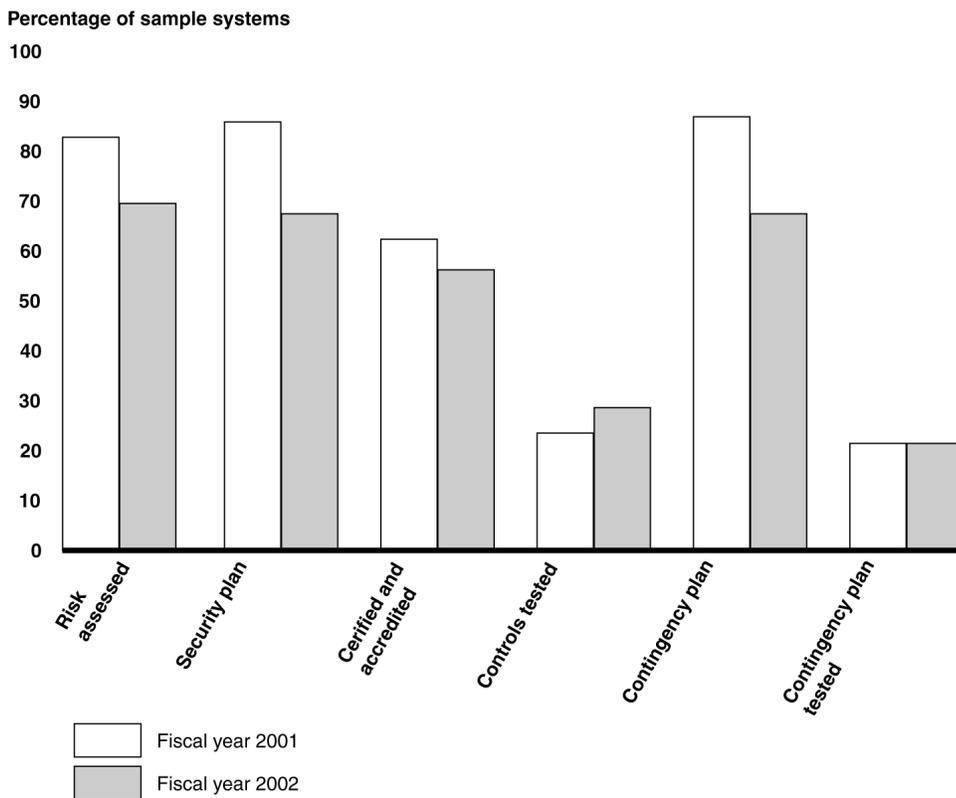
Percentage of sample systems

Fiscal year 2001

Fiscal year 2002

Systems Assessed for Risk

Agencies are required to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk management and overall security program management and, as our best

---

[26]U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003), and *Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements*, GAO-03-852T (Washington, D.C.: Jun. 24, 2003).

practice work has shown, are an integral part of the management processes of leading organizations.[27] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Our reviews of federal agencies, however, frequently show deficiencies related to assessing risk, such as security plans for major systems that are not developed on the basis of risk. As a result, the agencies had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable.

OMB's performance measure for this requirement mandated that agencies report the number and percentage of their systems that have been assessed for risk during fiscal year 2001 and fiscal year 2002. DOD reported that for its sample of 155 systems, 68 percent (106) had risk assessments for fiscal year 2002 as compared to 81 percent (125) for fiscal year 2001—a decrease of 13 percentage points. In comparison, our overall analyses of reporting for this measure for all 24 agencies (including DOD) showed that for fiscal year 2002, 11 agencies reported that they had assessed risk for 90 to 100 percent of their systems, and of the remaining 13, 8 reported less than 50 percent.

Systems With Up-to-Date Security Plans

An agency head is required to ensure that the agency's information security plans are practiced throughout the life cycle of each agency system. In its reporting instructions, OMB required agencies to report whether the agency head had taken specific and direct actions to oversee that program officials and the CIO are ensuring that security plans are up to date and practiced throughout the life cycle of each system. Agencies also had to report the number and percentage of systems that had an up-to-date security plan.

Regarding the status of agencies' security plans, DOD reported that for its sample of 155 systems, 66 percent (103) had up-to-date security plans for fiscal year 2002—a decrease from the 84 percent (130) reported for fiscal year 2001. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, 7 agencies reported that they up-to-date security plans for 90 to 100 percent of their systems, and of the remaining 17 agencies, 9 reported up-to-date security plans for less than 50 percent of their systems.

---

[27]GAO/AIMD-98-68.

Systems Certified and Accredited	As one of its performance measures for agency program official responsibilities, OMB required agencies to report the number and percentage of systems that have been authorized for processing following certification and accreditation. Certification is the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. Accreditation is the authorization of an IT system to process, store, or transmit information, granted by a management official that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. The accreditation decision is based on the implementation of an agreed upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it.

DOD has established a standard departmentwide process, set of activities, general tasks, and a management structure to certify and accredit information systems and maintain the IA and security posture throughout the life cycle of the system. A companion manual, the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, provides implementation guidance to standardize the certification and accreditation process throughout DOD.[28] The DOD CIO reported that the department is implementing the DITSCAP process, but realizes the actual process is complex, lengthy, and costly; and several internal agencies are exploring efforts to streamline DITSCAP.

DOD reported that for fiscal year 2002, 55 percent (85) of its sample of 155 systems was authorized for processing following certification and accreditation—a decrease from the 61 percent (95) reported for fiscal year 2001. For this particular measure, DOD also reported that in fiscal year 2002, 96 percent (352) of its 366-network sample was certified and accredited to operate. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, only 3 agencies reported that 90

---

[28]Department of Defense, *DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, DOD 8510.1-M (July 31, 2000).

to 100 percent of their systems were authorized for processing following certification and accreditation, and of the remaining 21 agencies, 13 reported that less than 50 percent of their systems were authorized, including 3 that reported that none were authorized.

According to the DOD IG's fiscal year 2002 GISRA report, the certification and accreditation data reported by the department for fiscal year 2001 included systems that were certified and accredited either under the DITSCAP or another process. In addition, in analyzing a sample of the systems used for the department's fiscal year 2001 GISRA reporting, the IG found the certification and accreditation status for some systems was incorrectly reported.

Security Control Testing and Evaluation

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

As a performance measure for this requirement, OMB required agencies to report the number and percentage of systems for which security controls have been tested and evaluated during fiscal years 2001 and 2002. DOD reported that for fiscal year 2002, it had tested and evaluated controls for only 28 percent (43) of the 155-system sample—a slight increase from the 23 percent (35) reported for fiscal year 2001. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, only 4 agencies reported they had tested and evaluated controls for 90 to 100 percent of their systems, and of the remaining 20 agencies, 10 reported less than 50 percent.

System Contingency Plans

Contingency plans provide specific instructions for restoring critical systems, including such items as arrangements for alternative processing facilities, in case the usual facilities are significantly damaged or cannot be accessed. These plans and procedures help to ensure that critical operations can continue when unexpected events occur, such as

temporary power failure, accidental loss of files, or major disaster. Contingency plans should also identify which operations and supporting resources are critical and need to be restored first and should be tested to identify their weaknesses. Without such plans, agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

As another of its performance measures, OMB required agencies to report the number and percentage of systems for which contingency plans had been prepared and had been tested in the past year. DOD reported that of its 155-system sample, 66 percent (103) of its systems had contingency plans for fiscal year 2002—a decrease from the 85 percent (131) reported for fiscal year 2001. However, more significantly, DOD also reported that for fiscal year 2002, only 21 percent (32) of its sample of systems had contingency plans that had been tested within the past year. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, only 2 agencies reported they had tested contingency plans for 90 to 100 percent of their systems, and of the remaining 22 agencies, 20 reported less than 50 percent, including 1 that reported none had been tested.

Incident-Handling Capabilities

Agencies are required to implement procedures for detecting, reporting, and responding to security incidents. Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management.

In March 2001, we reported that over the past several years, DOD had established incident response capabilities for the military services and enhanced computer defensive capabilities across the department.[29]

---

[29]U.S. General Accounting Office, *Information Security, Challenges to Improving DOD's Incident Response Capabilities*, GAO-01-341 (Washington, D.C.: Mar. 29, 2001).

However, we also identified six areas in which DOD faced challenges in improving its incident response capabilities, including (1) coordinating resource planning and priorities for incident response across the department; (2) integrating critical data from systems, sensors, and other devices to better monitor cyber events and attacks; (3) establishing a departmentwide process to periodically and systematically review systems and networks on a priority basis for security weaknesses; (4) ensuring that components across the department consistently and fully report compliance with vulnerability alerts; (5) improving the coordination and suitability of component-level incident response actions; and (6) developing departmentwide performance measures to assess incident response capabilities and thus better ensure mission readiness. Although DOD was aware of these challenges and had undertaken some initiatives to address them, the initiatives were not complete at the time of our review. We recommended that DOD act to address these challenges to better protect its systems and networks from cyber threats and attacks. Currently, DOD reports that it has made progress in addressing many of these challenges.

For fiscal year 2002 GISRA reporting, OMB required agencies to report several performance measures related to detecting, reporting, and responding to security incidents. These included the number of agency components with an incident-handling and response capability, whether the agency and its major components share incident information with the Federal Computer Incident Response Center (FedCIRC)[30] in a timely manner, and the numbers of incidents reported. OMB also required that agencies report on how they confirmed that patches have been tested and installed in a timely manner.

In its fiscal year 2002 GISRA report, the DOD CIO reported that essentially all its components have an incident handling and response capability and that DOD has made significant progress in developing its computer network defense capabilities, including the January 2001 issuance of DOD Directive O-8530.1, "Computer Network Defense," which established computer network defense policy, definition, and department responsibilities. The CIO also reported that through its computer network

---

[30]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide a central focal point for incident reporting, handling, prevention and recognition for the federal government.

defense capabilities, DOD could monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. In addition, the CIO reported that each of the major military services has a robust computer emergency response team (CERT) and integrated network operations centers. Further, the report states that the DOD CERT works closely with FedCIRC on all incidents within the .gov Internet domain and, along with other service and agency CERTs, shares incident information with FedCIRC within 10 minutes to 48 hours depending on the seriousness of the incident. The Joint Task Force for Computer Network Operations and the DOD CERT take responsibility for incidents within the .mil Internet domain.

In comparison to DOD, our analyses of agencies' fiscal year 2002 GISRA reports showed that most agencies reported that they have established incident-response capabilities. For example, 12 agencies reported that for fiscal year 2002, 90 percent or more of their components had incident handling and response capabilities, and 8 others reported that they provided these capabilities to components through a central point within the agency.

Security Training for Employees and Contractors

Agencies are required to provide training on security awareness for agency personnel and on security responsibilities for information security personnel. Our studies of best practices at leading organizations have shown that such organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools.

Among the performance measures for these requirements, OMB mandated that agencies report the number and percentage of employees—including contractors—who received security training during fiscal years 2001 and 2002, and the number of employees with significant security responsibilities who received specialized training. In response to these measures, the DOD CIO reported that it provides departmentwide, component-level security training and periodic updates for all employees, but that actual numbers and the percentage of agency employees who received security training in fiscal year 2002 were not available at the time of its report. For employees with significant security responsibilities, the CIO reported that specialized security and technical training is provided to persons empowered to audit, alter, or affect the intended behavior or content of an IT system, such as system/network administrators and

information systems security officers. Additional training is also provided for others, such as CERT members, computer crime investigators, and Web masters/site managers. However, performance measure data reported for employees with significant security responsibilities showed that of 39,783 such employees, 42 percent (16,812) received specialized training in fiscal year 2002—a decrease of 9 percentage points from the 51 percent reported for fiscal year 2001.

In comparison with other major federal agencies, for specialized training for employees with significant security responsibilities, our analyses showed that 12 agencies reported 50 percent or more of their employees with significant security responsibilities had received specialized training for fiscal year 2002, with 5 of these reporting 90 percent or more. Of the remaining 12 agencies, 9 including DOD reported that less than half of such employees received specialized training, 1 reported that none had received such training, and 2 did not provide sufficient data for this measure.

Security of Contractor-Provided Services

Agencies are required to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained by or for the agency. In its fiscal year 2001 GISRA report to the Congress, OMB identified poor security for contractor-provided services as a common weakness, and for fiscal year 2002 reporting, included performance measures to help indicate whether the agency program officials and CIO used appropriate methods, such as audits and inspections, to ensure that service provided by a contractor are adequately secure and meet security requirements.

For fiscal year 2002 GISRA, the DOD CIO reported that there was insufficient time and resources to accurately collect requested performance measure data. The CIO also reported that execution and verification of contractor services and facilities are managed at the subagency levels, and that agency program officials use audits or inspections to ensure that contractor-provided services are adequately secure and meet statutory information security requirements, OMB policy, and NIST guidance. The DOD IG did not review the status of contractor-provided services for compliance with GISRA, but did identify several reports issued from August 2001 to July 2002 by military service audit agencies that discussed weaknesses in background investigations. Screening of contractor or subcontractor employees as a condition for physical or computer systems access is a recommended safeguard, and depending on the program or system criticality or information sensitivity, can range from minimal checks to complete background investigations.

Challenges to Implementing an Effective Information Security Management Program

As previously discussed, our past analyses of audit results for 24 of the largest federal agencies showed that all 24 had significant weaknesses in security program management, which 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.[31] 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.[32] Our study found that these organizations managed their information security risks through a cycle of risk management activities. These activities, which are now among the federal government's statutory information security requirements, included

- assessing risks and determining protection needs, selecting and implementing cost-effective policies and controls to meet those 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.

Although GISRA reporting provided performance information on these areas, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security. Also, developing management strategies that identify

---

[31] GAO-02-231T and GAO-03-303T.

[32] GAO/AIMD-98-68.

specific actions, time frames, and required resources may help to significantly improve performance.

In January 1998, DOD announced its plans for DIAP—a program intended to promote integrated, comprehensive, and consistent IA practices across the department. In February 1999, the department issued an approved implementation plan, which described, at a high level, the program's goals, objectives, and organizational structure, and confirmed its responsibility for the planning, coordination, integration, and oversight of Defense-wide computer security initiatives.

In March 2001, we reported that DIAP had made progress in addressing IA, but that the department had not yet met its goals for promoting integrated, comprehensive, and consistent practices across DOD.[33] The program's progress was limited by weaknesses in its management framework and unmet staffing expectations. DOD had not established a performance-based management framework for IA improvement at the department level. As a result, DOD was unable to accurately determine the status of IA across the department, the progress of its improvement efforts, or the effectiveness of its initiatives. Also, understaffing kept the program from fulfilling its central role in planning, monitoring, coordinating, and integrating Defense-wide IA activities, and changes in the composition and authority of other key organizations interacting with DIAP left it without a consistent and fully supportive environment for its operations. We concluded that achieving this program's vision for information superiority would require the commitment of DOD to proven IA management practices. To improve progress toward the department's goals, we made recommendations to the Secretary of Defense in the areas of component commitments to DIAP and executive-level monitoring of the program. We also recommended that the DOD CIO institute performance-based management of DIAP through a defined budget and performance objectives, and that the program manager take steps to address the program's unmet goals.

DOD has made some progress in addressing our previous recommendations and, as discussed previously, during fiscal year 2003,

---

[33]U.S. General Accounting Office, *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program*, GAO-01-307 (Washington, D.C.: Mar. 30, 2001).

DOD issued guidance to establish policy and assign responsibility for IA management and to prescribe a framework for implementing the department's IA program and establish baseline levels of assurance for information systems. Despite such steps, OMB reported in its fiscal year 2002 report to the Congress that the overall results of the Defense audit community's assessment of the DOD fiscal year 2001 GISRA reporting reinforced the position that DOD does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and ensuring that those policies are consistently practiced throughout the department.

In summary, DOD has taken positive steps through its policy and guidance to establish information security as a priority for the department. However, as its fiscal year 2002 GISRA reporting showed, further effort is needed to fully implement statutory information security requirements departmentwide and to expand future FISMA reporting to all systems. Significant improvement will likely require DOD to establish departmentwide processes that routinely provide information for day-to-day management of information security and to develop management strategies that identify specific actions, time frames, and required resources. With the first agency reporting under FISMA due in September 2003, updated information on the status of DOD's efforts will be available for continued congressional oversight.

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.