United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at
9:30 a.m. EDT
Thursday,
April 5, 2001

COMPUTER SECURITY

Weaknesses Continue to Place Critical Federal Operations and Assets at Risk

Statement of Robert F. Dacey
Director, Information Security Issues

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our analysis of information security audits 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, data tampering, fraud, and inappropriate disclosure of sensitive information.

Today, I will summarize the results of our analysis of information security audits performed by us and by agency inspectors general since July 1999 at 24 major federal departments and agencies. In summarizing these results, I will discuss the types of pervasive weaknesses that we and agency inspectors general have identified. I will then describe the serious risks that these weaknesses pose at selected individual agencies of particular interest to this subcommittee, and the major common weaknesses that agencies need to address. Finally, I will describe the management improvements that are needed to resolve these weaknesses and the significant challenges that remain.

Background

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

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, 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.

Reports of attacks and disruptions abound. The March 2001 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the Federal Bureau of Investigation's San Francisco Computer Intrusion Squad, showed that 85 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. Disruptions caused by virus attacks, such as the ILOVEYOU virus in May 2000 and 1999's Melissa virus, have illustrated the potential for damage that such attacks hold.[1] A sampling of reports summarized in Daily Reports by the FBI's National Infrastructure Protection Center[2] during two recent weeks in March illustrates the problem further:

- Hackers suspected of having links to a foreign government successfully broke into the Sandia National Laboratory's computer system and were able to access sensitive classified information.(Source: Washington Times, March 16, 2001.)

- A hacker group by the name of "PoizonB0x" defaced numerous government web sites, including those of the Department of Transportation, the Administrative Office of the U.S. Courts, the National Science Foundation, the National Oceanic and Atmospheric Administration, the Princeton Plasma Physics Laboratory, the General Services Administration, the U.S. Geological Survey, the Bureau of Land Management, and the Office of Science & Technology Policy. (Source: Attrition.org., March 19, 2001.)

- The "Russian Hacker Association" is offering over the Internet an e-mail bombing system that will destroy a persons "web enemy" for a fee. (Source: UK Ministry of Defense Joint Security Coordination Center)

- Two San Diego men allegedly crashed a company's computer system by rerouting tens of thousands of unsolicited e-mails through its servers. (Source: ZDNet News, March 18, 2001.)

---

[1] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000); *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000); *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

[2] In its Daily Reports, the National Infrastructure Protection Center states that these summaries are for information purposes only and do not constitute any verification of the information contained in the reports or endorsement by the FBI.

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

Since 1996, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from these threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September 1996, we reported that serious weaknesses had been found at 10 of the 15 largest federal agencies, and we concluded that poor information security was a widespread federal problem with potentially devastating consequences.[3] In 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies: both analyses found that all 24 agencies had significant information security weaknesses.[4] As a result of these analyses, we have identified information security as a high-risk issue in reports to the Congress since 1997—most recently in January 2001.[5]

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

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

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

Weaknesses Remain Pervasive

Evaluations published since July 1999 show that federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk. Significant weaknesses have been identified in each of the 24 agencies covered by our review. These weaknesses 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 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.

Weaknesses in these areas placed a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they placed an enormous amount of highly sensitive data—much of it pertaining to individual taxpayers and beneficiaries—at risk of inappropriate disclosure.

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. While these increases in reported weaknesses are disturbing, they 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, our analysis leaves 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 covered in our analysis were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits may provide a less complete picture of the agency's overall security

posture because the audit objectives focused on the financial statements and did not include evaluations of systems supporting nonfinancial operations.

In response to congressional interest, during fiscal years 1999 and 2000, we expanded our audit focus to cover a wider range of nonfinancial operations. We expect this trend to continue.

Risks to Federal Operations, Assets, and Confidentiality Are Substantial

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

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

Such risks, if inadequately addressed, may limit government's ability to take advantage of new technology and improve federal services through electronic means. For example, this past February, we reported on serious control weaknesses in the Internal Revenue Service's (IRS) electronic filing system, noting that failure to maintain adequate security could erode public confidence in electronic filing, jeopardize the Service's ability to meet its goal of 80 percent of returns being filed electronically by 2007, and deprive it of financial and other anticipated benefits. Specifically, we found that, during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both internal and external to IRS, could have gained access to these systems and viewed, copied,

modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electonic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS has completed corrective action for all of the critical access control vulnerabilities we identified and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.[6] As part of our audit follow up activities, we plan to evaluate the effectiveness of IRS's corrective actions.

I would now like to describe the risks associated with specific recent audit findings at agencies of particular interest to this subcommittee.

- Information technology is essential to the Department of Energy's (DOE) scientific research mission, which is supported by a large and diverse set of computing systems, including very powerful supercomputers located at DOE laboratories across the nation. In June 2000, we reported that computer systems at DOE laboratories supporting civilian research had become a popular target of the hacker community, with the result that the threat of attacks had grown dramatically in recent years.[7] Further, because of security breaches, several laboratories had been forced to temporarily disconnect their networks from the Internet, disrupting the laboratories' ability to do scientific research for up to a full week on at least two occasions. In February 2001, the DOE's Inspector General reported network vulnerabilities and access control weaknesses in unclassified systems that increased the risk that malicious destruction or alteration of data or the processing of unauthorized operations could occur.[8]

- In February, the Department of Health and Human Services' Inspector General again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[9] Most significant were weaknesses associated with the department's Health Care Financing Administration, which was responsible, during fiscal year

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

[7] *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/AIMD-00-140, June 9, 2000).

[8] *Report on the Department of Energy's Consolidated Financial Statements*, DOE/IG-FS-01-01, February 16, 2001.

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

2000, for processing more than $200 billion in medicare expenditures. HCFA relies on extensive data processing operations at its central office to maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and to process all payments for managed care. HCFA also relies on Medicare contractors, who use multiple shared systems to collect and process personal health, financial, and medical data associated with Medicare claims. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

- The Environmental Protection Agency (EPA) relies on its computer systems to collect and maintain a wealth of environmental data under various statutory and regulatory requirements. EPA makes much of its information available to the public through Internet access in order to encourage public awareness of and participation in managing human health and environmental risks and to meet statutory requirements. EPA also maintains confidential data from private businesses, data of varying sensitivity on human health and environmental risks, financial and contract data, and personal information on its employees. Consequently, EPA's information security program must accommodate the often competing goals of making much of its environmental information widely accessible while maintaining data integrity, availability, and appropriate confidentiality. In July 2000, we reported serious and pervasive problems that essentially rendered EPA's agencywide information security program ineffective.[10] Our tests of computer-based controls concluded that the computer operating systems and agencywide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses.

  In addition, EPA's records showed that its vulnerabilities had been exploited by both external and internal sources, as illustrated by the following examples.

  - In June 1998, EPA was notified that one of its computers was used by a remote intruder as a means of gaining unauthorized access to a state university's computers. The problem report stated that vendor-supplied software updates were available to correct the vulnerability, but EPA had not installed them.

[10] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215, July 6, 2000).

- In July 1999, a chat room was set up on a network server at one of EPA's regional financial management centers for hackers to post notes and, in effect, conduct on-line electronic conversations.

- In February 1999, a sophisticated penetration affected three of EPA's computers. EPA was unaware of this penetration until notified by the FBI.

- In June 1999, an intruder penetrated an Internet web server at EPA's National Computer Center by exploiting a control weakness specifically identified by EPA about 3 years earlier during a previous penetration of a different system. The vulnerability continued to exist because EPA had not implemented vendor software updates (patches), some of which had been available since 1996.

- On two occasions during 1998, extraordinarily large volumes of network traffic—synonymous with a commonly used denial-of-service hacker technique—affected computers at one of EPA's field offices. In one case, an Internet user significantly slowed EPA's network activity and interrupted network service for over 450 EPA computer users. In a second case, an intruder used EPA computers to successfully launch a denial-of-service attack against an Internet service provider.

- In September 1999, an individual gained access to an EPA computer and altered the computer's access controls, thereby blocking authorized EPA employees from accessing files. This individual was no longer officially affiliated with EPA at the time of the intrusion, indicating a serious weakness in EPA's process for applying changes in personnel status to computer accounts.

Of particular concern was that many of the most serious weaknesses we identified—those related to inadequate protection from intrusions through the Internet and poor security planning—had been previously reported to EPA management in 1997 by EPA's inspector general.[11] The negative effects of such weaknesses are illustrated by EPA's own records, which show several serious computer security incidents since early 1998 that have resulted in damage and disruption to agency operations. As a result of these weaknesses, EPA's computer systems and the operations that rely on them were highly vulnerable to tampering, disruption, and misuse from both internal and external sources.

[11] *EPA's Internet Connectivity Controls,* Office of Inspector General Report of Audit (Redacted Version), September 5, 1997.

EPA management has developed and begun to implement a detailed action plan to address reported weaknesses. However, the agency does not expect to complete these corrective actions until 2002 and continued to report a material weakness in this area in its fiscal year 2000 report on internal controls under the Federal Managers' Financial Integrity Act of 1982.[12]

- The Department of Commerce is responsible for systems that the department has designated as critical for national security, national economic security, and public health and safety. Its member bureaus include the National Oceanic and Atmospheric Administration, the Patent and Trademark Office, the Bureau of the Census, and the International Trade Administration. During December 2000 and January 2001, Commerce 's inspector general reported significant computer security weaknesses in several of the department's bureaus and, last month, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements. These included a lack of formal, current security plans and weaknesses in controls over access to systems and over software development and changes.[13] At the request of the full committee, we are currently evaluating information security controls at selected other Commerce bureaus.

While Nature of Risk Varies, Control Weaknesses Across Agencies Are Strikingly Similar

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

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any

[12] *Audit Report on EPA's Fiscal 2000 Financial Statements*, Office of the Inspector General Audit Report 2001-1-00107, February 28, 2001.

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

identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than react to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Virtually all of the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not developed security plans for major systems based on risk, had not documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, 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 controls that were not effective, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

With the October 2000 enactment of the government information security reform provisions of the fiscal year 2001 National Defense Authorization Act, agencies are now required by law to adopt the practices described above, including annual management evaluations of agency security.

Access Controls

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

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 to 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 terminated employees, and changes in users' responsibilities and related access needs.

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

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled; neither were they adjusted for those whose responsibilities, and thus need to access certain files, changed. At one agency, as a result, former employees and contractors could and in many cases did still read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.

- Users were not required to periodically change their passwords.

- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At another agency, 20,000 users had been provided access to one system without written authorization.

- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.

- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the capability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

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

Application Software Development and Change Controls

Application software development and change controls 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 prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and to ensure that different versions are not misidentified.

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

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

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

Segregation of Duties

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

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

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

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a combination of physical and logical access controls and by effective supervisory review.

Segregation of duties weaknesses were identified at most of the agencies covered by our analysis. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff members involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt-recorded by the same individual.

Operating System 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 of the applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of

the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosure. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them.

Weaknesses were identified at each of the agencies for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

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

Service Continuity

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations, should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. If 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 financial or management information. Controls to ensure service continuity should address the entire range of potential disruptions. These may include 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.

Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity control weaknesses were reported for most of the agencies covered by our analysis. Examples of weaknesses included the following:

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

Improved Security Program Management Is Essential

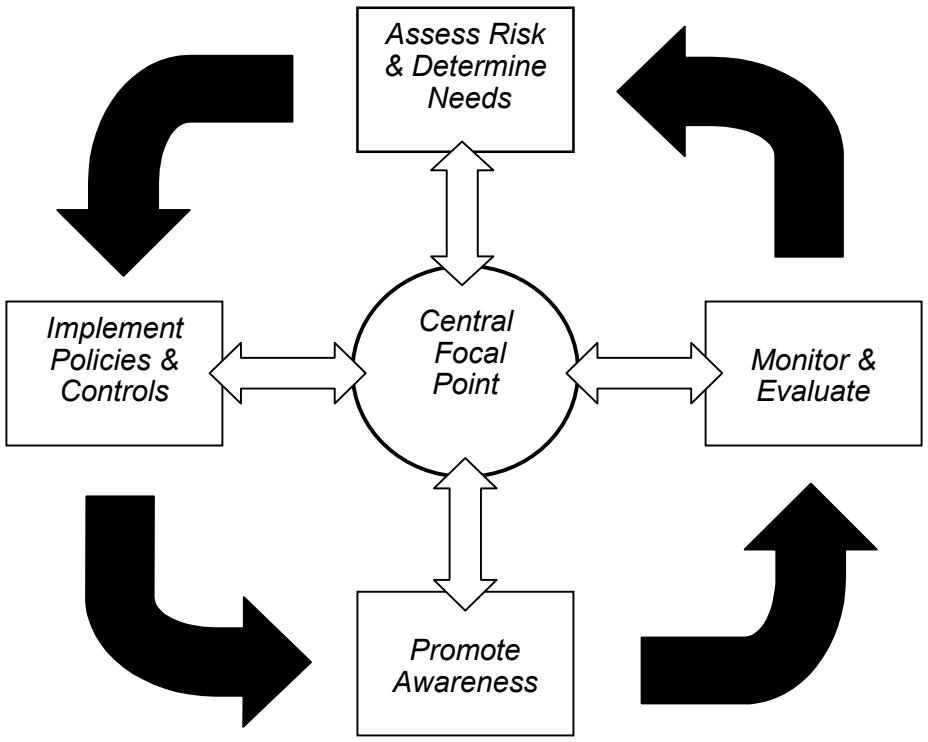
The audit reports cited in this statement and in our prior information security reports include many recommendations to individual agencies that address specific weaknesses in the areas I have just described. It is each individual agency's responsibility to ensure that these recommendations are implemented. Agencies have taken steps to address problems and many have good remedial efforts underway. However, these efforts will not be fully effective and lasting unless they are supported by a strong agencywide security management framework.

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

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

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

Figure 1: Risk Management Cycle



This cycle of activity, as described in our May 1998 executive guide, is consistent with guidance on information security program management provided to agencies by the Office of Management and Budget (OMB) and by NIST. In addition, the guide has been endorsed by the federal Chief Information Officers (CIO) Council as a useful resource for agency managers. We believe that implementing such a cycle of activity is the key to ensuring that information security risks are adequately considered and addressed on an ongoing basis.

While instituting this framework is essential, there are several steps that agencies can take immediately. Specifically, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their

best practices, and (6) ensure that their most common vulnerabilities are addressed. None of these actions alone will ensure good security. However, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay.

New Legal Requirements Provide Basis for Improved Management and Oversight

Due to concerns about the repeated reports of computer security weaknesses at federal agencies, in 2000, the Congress passed government information security reform provisions require agencies to implement the activities I have just described. These provisions were enacted in late 2000 as part of the fiscal year 2001 NationalDefense Authorization Act. In addition to requiring these management improvements, the new provisions require annual evaluations of agency information security programs by both management and agency inspectors general. The results of these reviews, which are initially scheduled to become available in late 2001, will provide a more complete picture of the status of federal information security than currently exists, thereby providing the Congress and OMB an improved means of overseeing agency progress and identifying areas needing improvement.

Improvement Efforts Are Underway, but Many Challenges Remain

During the last two years, a number of improvement efforts have been initiated. Several agencies have taken significant steps to redesign and strengthen their information security programs; the Federal Chief Information Officers Council has issued a guide for measuring agency progress, which we assisted in developing; and the President issued a National Plan for Information Systems Protection and designated the related goals of computer security and critical infrastructure protection as a priority management objective in his fiscal year 2001 budget. These actions are laudable. However, recent reports and events indicate that they are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks.

While OMB, the Chief Information Officers Council, and the various federal entities involved in critical infrastructure protection have expanded their efforts, it will be important to maintain the momentum. As we have noted in previous reports and testimonies, there are actions that can be taken on a governmentwide basis to enhance agencies' abilities to implement effective information security.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal

agency security; and NIST, with assistance from the National Security Agency (NSA), is responsible for establishing related standards. In addition, interagency bodies, such as the CIO Council and the entities created under Presidential Decision Directive 63 on critical infrastructure protection are attempting to coordinate agency initiatives. While these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not taking place, and it is unclear 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 they enforce these controls. In theory, this 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.

However, our studies of best practices at leading organizations have shown that more specific guidance is important. 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; and help ensure that shared data are appropriately protected. 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 information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

Third, routine periodic audits, such as those required in the government information security reforms recently enacted, would allow for more meaningful performance measurement. Ensuring effective implementation of agency information security and critical infrastructure protection plans will require monitoring to determine if milestones are being met and testing to determine if policies and controls are operating as intended.

Fourth, the Congress and the executive branch can use of audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential to

holding agencies accountable for their performance as was demonstrated by the OMB and congressional efforts to oversee the year 2000 computer challenge.

Fifth, it is important for agencies to have the technical expertise they need to select, implement, and maintain controls that protect their computer systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. As the year 2000 challenge showed, the availability of adequate technical expertise has been a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their computer security and infrastructure protection activities. 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, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on computer security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes not supported by a strong agency risk management framework.

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

Contact and Acknowledgments

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.*

(310118)