



Testimony

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

COMPUTER SECURITY

November 9, 2001

Improvements Needed to Reduce Risk to Critical Federal Operations and Assets

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 recent information security audits and evaluations at federal agencies. As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information.

Our analyses covers information security audits and evaluations that we and agency inspectors general (IGs) performed since July 2000 at 24 major federal departments and agencies. In summarizing these results, I will discuss the continuing pervasive weaknesses that led GAO to initially begin reporting information security as a governmentwide high-risk issue in 1997. I will then illustrate the serious risks that these weaknesses pose at selected individual agencies and also describe the major common weaknesses that agencies need to address to improve their information security programs. Finally, I will discuss the importance of establishing a strong agencywide security management program in each agency and developing a comprehensive governmentwide strategy for improvement.

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 24 hours a day; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with virtually an unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services all depend on the security of their computer operations. Likewise, the speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere

with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

Reports of attacks and disruptions are growing. The number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 21,756 in 2000 and 34,754 for just the first 9 months of 2001.¹ And these are only the *reported* attacks. The CERT® Coordination Center estimates that as much as 80 percent of actual security incidents go unreported, in most cases because the organization was unable to recognize that its systems had been penetrated or because there were no indications of penetration or attack. As the number of individuals with computer skills has increased, more intrusion or “hacking” tools have become readily available and relatively easy to use. A potential hacker can literally download tools from the Internet and “point and click” to start a hack. According to a recent National Institute of Standards and Technology (NIST) publication, hackers post 30 to 40 new tools to hacking sites on the Internet every month.

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.

Attacks over the past several months illustrate the risks. As we reported to this Subcommittee in August 2001, the attacks referred to as Code Red, Code Red II, and SirCam have affected millions of computer users, shut down web sites, slowed Internet service, and disrupted business and government operations, and have reportedly caused billions of dollars in damage.² More recently, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999’s infamous Melissa virus, allowing it to spread widely in a short amount of time.³

¹CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

²*Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* (GAO-01-1073T, August 29, 2001).

³*Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Virus*: a program that “infects” computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the “infected” file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.

As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. Government officials have long been concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, worms, Trojan horses, logic bombs, and eavesdropping sniffers that can destroy, intercept, or degrade the integrity of and deny access to data.⁴ In addition, the disgruntled organization insider is a significant threat, since such individuals with little knowledge about computer intrusions often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets. Examples of such attacks already exist:

- In October 2000, the FBI's National Infrastructure Protection Center (NIPC) issued an advisory concerning an increased level of cyber activity against web sites related to Israel and pro-Palestinian organizations. This advisory noted that due to the credible threat of terrorist acts in the Middle East region, and the conduct of these web attacks, increased vigilance should be exercised to the possibility that U.S.-government and private-sector web sites may become potential targets. In less than a month, a group of hackers calling itself Gforce Pakistan defaced more than 20 web sites and posted threats to launch an Internet attack against AT&T. Further, in October 2001, this same group attacked a government web server operated by the National Oceanic and Atmospheric Administration, defacing a web site and threatening to release some highly confidential data unless the United States met several demands.
- According to recent Defense Intelligence Agency and Central Intelligence Agency estimates, at least 20 countries are known to be developing information warfare strategies that specifically target U.S. military and private-sector data networks. The fear is that computer viruses and worms

⁴*Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

unleashed by foreign hackers could wreak havoc on the U.S. infrastructure in the event of a military conflict.

- In his April 2001 written statement for the House Energy and Commerce Committee on intrusions into government computer networks, the director of the NIPC noted that terrorist groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely.⁵ Citing the example of convicted terrorist Ramzi Yousef, who masterminded the 1993 World Trade Center bombing and stored detailed plans to destroy U.S. airliners in encrypted files on his laptop computer, the director concluded that while we have not yet seen terrorist groups employ cyber tools as a weapon against critical infrastructures, the reliance of these groups on information technology and acquisition of computer expertise are clear warning signs.

After the September 11, 2001, attacks, the NIPC warned of an expected upswing in incidents and encouraged system administrators to follow best practices to limit the potential damage from any cyber attacks. In particular, it warned that political events and international situations would likely lead to increasing cyber protests and that such attacks were expected to now target the information infrastructure more often and exploit opportunities to disrupt or damage it. On November 2, the NIPC updated its warning, noting that hacking groups have formed and participated in pro-U.S. and anti-U.S. cyber activities, which have mainly taken the form of web defacements. The NIPC went on to say that while there has been minimal activity in the form of denial-of-service attacks, it has reason to believe that the potential for such attacks in the future is high and that infrastructure support systems must take a defensive posture and remain at a higher state of alert.

Finally, while the warning of a potential “digital Pearl Harbor” has been raised in the past, the events of September 11, 2001, further underscored the need to protect America’s cyberspace against potentially disastrous cyber attacks. In his September 2001 testimony before this Subcommittee on cyber attacks, the former NIPC director warned that a cyber attack by terrorists or nation-states using multiple-attack scenarios could have disastrous effects on infrastructure systems and could also be coordinated to coincide with physical terrorist attacks to maximize the impact of both. Further, in his October congressional testimony, Governor James Gilmore,

⁵“Issue of Intrusions into Government Computer Networks,” Statement for the Record by Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation before the House Energy and Commerce Committee, Oversight and Investigation Subcommittee, April 5, 2001.

Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (commonly known as the “Gilmore Commission”), cautioned that our critical information and communication infrastructures are targets for terrorists because of the broad economic and operational consequences of a shutdown.⁶ He warned that systems and services critical to the American economy and the health of our citizens—such as banking and finance, “just-in-time” delivery system for goods, hospitals, and state and local emergency services—can all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.

Weaknesses in Federal Systems Remain Pervasive

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.⁷ Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 agencies had significant information security weaknesses.⁸ As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.⁹

Our most recent analyses, of reports published from July 2000 through September 2001, continue to show significant weaknesses in federal

⁶Testimony of Governor James S. Gilmore III, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction before the House Science Committee, October 17, 2001.

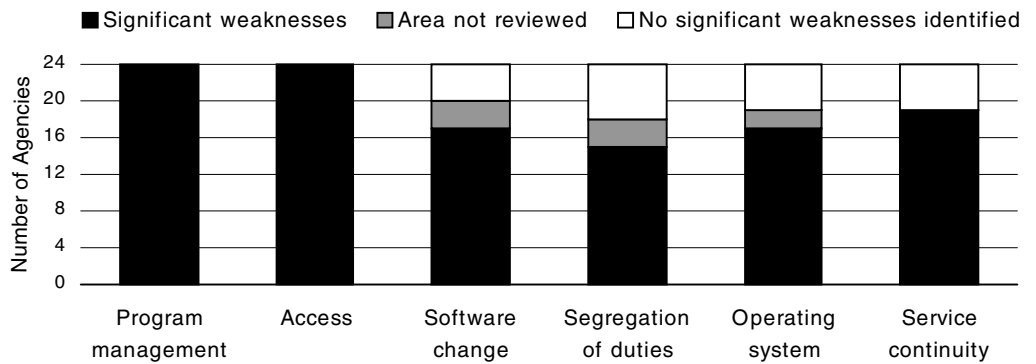
⁷*Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

⁸*Information Security: Serious Weaknesses Place Critical Federal 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).

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

computer systems that put critical operations and assets at risk.¹⁰ Weaknesses continued to be reported in each of the 24 agencies included in our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity’s information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems 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 1 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 1: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued July 2000 through September 2001.

As in 2000, our current analysis shows that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as 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

¹⁰These reports include the independent IG evaluations of agencies’ information security programs required by the Government Information Security Reform provisions of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398).

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 also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

In 2001, we also found weaknesses at 19 of the 24 agencies (79 percent) in service continuity controls (compared to 20 agencies or 83 percent in 2000). These controls 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.

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

Most of the audits represented in figure 1 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 (DOD) 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 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 is also likely to increase as agencies review and evaluate their information security programs as required by government information security reform provisions.¹¹ These provisions require agencies to implement security program management improvements, perform annual management reviews, have independent IG evaluations of agencies' information security programs, and report the results of these reviews and evaluations to the Office of Management and Budget (OMB). As I will discuss later in my testimony, the first reports under these new provisions were submitted to OMB in September 2001.

Information security weaknesses are also indicated by limited agency progress in implementing Presidential Decision Directive (PDD) 63 to protect our nation's critical infrastructures from computer-based attacks.¹² A March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in agencies' implementation of PDD 63 based on reviews conducted by agency IGs.¹³ This report concluded that the federal government could improve its PDD 63 planning and assessment activities and questioned the federal government's ability to protect the nation's critical infrastructures from intentional destructive acts by May 2003, as required in PDD 63. Specifically, the report stated that

- many agency critical infrastructure protection plans were incomplete, and some agencies had not developed such plans,
- most agencies had not completely identified their mission-essential infrastructure assets, and

¹¹P.L. 106-398.

¹²Issued in May 1998, Presidential Decision Directive (PDD) 63 called for a range of activities to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious attacks. The directive established critical infrastructure protection as a national goal, stating that, by the close of 2000, the United States was to have achieved an initial operating capability and, no later than 2003, the capability to protect the nation's critical infrastructures from intentional destructive acts.

¹³The PCIE primarily comprises the presidentially appointed inspectors general (IGs) and the ECIE primarily comprises IGs appointed by agency heads. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 IGs of their respective agencies' PDD 63 planning and assessment activities.

-
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective IG reviews.¹⁴ For example, whereas five agencies had or were in the process of updating their plans, three were not revising their plans to address reported deficiencies. In addition, although most of the agencies we reviewed had identified critical assets, many had not completed related vulnerability assessments. Further, most of the eight agencies we reviewed had not taken the additional steps to identify interdependencies and, as a result, some agency officials said that they were not sure which of their assets were critical from a national perspective and, therefore, subject to PDD 63. Identifying interdependencies is important so that infrastructure owners can determine when disruption in one infrastructure could result in damage to other infrastructures.

Substantial Risks Persist for Federal Operations, Assets, and Confidentiality

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

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

- resources, such as federal payments and collections, could be lost or stolen;
- 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 or browsed or copied for purposes of espionage or other types of crime;

¹⁴*Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

-
- 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.

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

- In August, we reported that significant and pervasive weaknesses placed Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.¹⁵ Commerce's IG has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.¹⁶
- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than \$12 billion annually in payments that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.¹⁷
- In March, we reported that although DOD's Departmentwide Information Assurance Program made progress, it had not yet met its goals of

¹⁵*Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk* (GAO-01-751, August 13, 2001).

¹⁶*Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements*, Inspector General Audit Report No. FSD-12849-1-0001.

¹⁷*Information Security: Weak Controls Place Interior's Financial and Other Data at Risk* (GAO-01-615, July 3, 2001).

integrating information assurance with mission-readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.¹⁸

- In February, the Department of Health and Human Services' IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.¹⁹ Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which, during fiscal year 2000, was responsible for processing more than \$200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data (such as Medicare enrollment, eligibility, and paid claims data) and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

To correct reported weaknesses, several agencies took significant steps to redesign and strengthen their information security programs. For example, the Internal Revenue Service (IRS) made notable progress in improving computer security at its facilities, corrected a significant number of identified weaknesses, and established a servicewide computer security management program that, when fully implemented, should help the agency effectively manage its security risks.²⁰ Similarly, the Environmental Protection Agency has moved aggressively to reduce the exposure of its systems and data and to correct weaknesses we identified in February 2000.²¹ While we have not tested their effectiveness, these actions show that the agency is taking a comprehensive and systematic approach that should help ensure that its efforts are effective.

¹⁸*Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, March 30, 2001).

¹⁹*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.

²⁰*Financial Audit: IRS' Fiscal Year 1999 Financial Statements* (GAO/AIMD-00-76, February 29, 2000).

²¹*Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215, July 6, 2000).

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

Specifically, we found that during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both within and outside IRS, could have gained access to these systems and viewed, copied, modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electronic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS completed corrective action for all the critical access control vulnerabilities we identified before the 2001 filing season and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.²²

Addressing weaknesses such as those we identified in the IRS' electronic filing system is especially important in light of the administration's plans to improve government services by expanding use of the Internet and other computer-facilitated operations—collectively referred to as electronic government, or E-government.²³ Specific initiatives proposed for fiscal year 2002 include expanding electronic means for (1) providing information to citizens, (2) handling procurement-related transactions, (3) applying for and managing federal grants, and (4) providing citizens information on the development of specific federal rules and regulations. Anticipated benefits include reducing the expense and difficulty of doing business with the government, providing citizens improved access to government services, and making government more transparent and accountable. Success in achieving these benefits will require agencies and others involved to ensure that the systems supporting E-government are protected from fraud, inappropriate disclosures, and disruption. Without this protection, confidence in E-government may be diminished, and the related benefits never fully achieved.

²²Information Security: IRS Electronic Filing Systems (GAO-01-306, February 16, 2001).

²³The President's Management Agenda, Fiscal Year 2002, www.whitehouse.gov/omb/budget.

Similar Control Weaknesses Continue Across Agencies

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

Security Program Management

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

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed security plans for major systems based on risk, (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

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

Access Controls

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

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

Significant access control weaknesses that we have commonly identified include the following:

- Accounts and passwords for individuals no longer associated with an agency are not deleted or disabled or are not adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, in some cases, former employees and contractors could still and in many cases did read, modify, copy, or delete data; and even after long periods of inactivity, many users' accounts had not been deactivated.
- Users are not required to periodically change their passwords.
- Managers do not precisely identify and document access needs for individual users or groups of users. Instead, they provide overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. For example, in some cases, large numbers of users were granted access to sensitive system

directories and settings or provided access to systems without written authorization.

- Use of default, easily guessed, and unencrypted passwords significantly increases the risk of unauthorized access. We are often able to guess many passwords based on our knowledge of commonly used passwords and to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Software access controls are improperly implemented, resulting in unintended access or gaps in access-control coverage. For example, in some cases, excessive numbers of users, including programmers and computer operators, had the ability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. In addition, 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. In almost every test, our auditors have been successful in readily gaining unauthorized access that would allow both internal and external intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. Much of the activity associated with our intrusion testing had not been recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Software Development and Change Controls

Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled

libraries to protect them from unauthorized changes and different versions are not misidentified.

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

Examples of weaknesses in this area include the following:

- Testing procedures are undisciplined and do not ensure that implemented software operates as intended. For example, systems were sometimes authorized for processing without testing access controls to ensure that they had been implemented and were operating effectively. Also, documentation was not always retained to demonstrate user testing and acceptance.
- Implementation procedures do not ensure that only authorized software is used. In particular, procedures do not ensure that emergency changes are subsequently tested and formally approved for continued use and that implementation of “locally developed” (unauthorized) software programs is prevented or detected.
- Agencies’ policies and procedures frequently do not address the maintenance and protection of program libraries.

Segregation of Duties

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

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

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

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Segregation of duties can be enforced by a combination of physical and logical access controls and by effective supervisory review. Common problems involve computer programmers and operators who are authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. An example of this would be a single individual authorized to independently develop, test, review, and approve software changes for implementation.

We also identified segregation-of-duties problems related to transaction processing. For example, we found staff members involved with procurement who had system access privileges, allowing them to individually request, approve, and record the receipt of purchased items. In addition, we found staff members with 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.

Operating System Software Controls

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

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

The control concerns for system software are similar to the access control issues and software program change control issues previously discussed. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. A common type of problem reported is insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, we found system support personnel that 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 subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

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

Service Continuity Controls

Finally, the terrorist events that began on September 11, 2001, have redefined the disasters that must be considered in identifying and implementing service continuity controls to ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service

continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

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

To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. Agencies should then take steps to prevent and minimize potential damage and interruption. These steps include routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage; installing environmental controls, such as fire suppression systems or backup power supplies; arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and ensuring that staff and other users of the system understand their responsibilities in case of emergencies. Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it

should be communicated to affected staff. The plan should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location²⁴ and travel and lodging for necessary personnel, off-site storage location for backup files, and procedures for restoring critical applications and their order in the restoration process. In testing the plan, it is most useful to simulate a disaster situation that tests overall service continuity, including whether the alternative data processing site functions as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Such testing not only helps managers identify weaknesses, it also assesses how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred.

Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. Federal agencies depend not only on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency. As we reported in September 2000 on the lessons learned from this challenge, developing these plans was one of a number of management practices that, if continued, could improve federal agencies' overall information technology management, particularly in areas such as critical infrastructure protection and security.²⁵

In the aftermath of the September 11, 2001, attacks, news reports indicate that business continuity and contingency planning has been a critical factor in restoring operations for New York's financial district, with some specifically attributing companies' preparedness to the contingency

²⁴Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors, such as making arrangements with suppliers of computer hardware and telecommunications services, as well as with suppliers of business forms and other office supplies.

²⁵*Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges* (GAO/AIMD-00-290, September 12, 2000).

planning efforts begun for the Year 2000 challenge. In particular, the Year 2000 challenge increased management attention on continuity and risk management. It also gave companies a chance to rehearse a disaster beforehand. However, whereas the Year 2000 challenge may have increased the focus on business continuity and contingency planning, our analyses show that most federal agencies currently have service continuity control weaknesses. Examples of common agency weaknesses include the following:

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

Agencies Can Take Immediate Steps to Improve Security Program Management

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

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

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

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

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

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

Improvement Efforts Are Underway, But Challenges Remain

During the last 2 years, a number of improvement efforts have been initiated. As mentioned previously, several agencies have taken significant steps to redesign and strengthen their information security programs. In addition, the Federal Chief Information Officers (CIO) 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 in January 2000.

More recently, partially in response to the events of September 11, 2001, the President created the Office of Homeland Security with duties that include coordinating efforts to protect critical public and private information systems within the United States from terrorist attack. The President also appointed a Special Advisor for Cyberspace Security to coordinate interagency efforts to secure information systems and created the

President's Critical Infrastructure Protection Board to recommend policies and coordinate programs for protecting information for critical infrastructure. The Board is to include a standing committee for executive branch information systems security, chaired by an OMB designee.

These actions are laudable. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed in the context of the broader array of risks to the nation's welfare.

Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement. In 1998, shortly after the initial issuance of PDD 63, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the Assistant to the President for National Security Affairs work together to ensure that the roles of new and existing federal efforts were coordinated under a comprehensive strategy.²⁶ Our more recent reviews of the NIPC and of broader federal efforts to counter computer-based attacks showed that there was a continuing need to clarify responsibilities and critical infrastructure protection objectives.²⁷ As the administration refines the strategy that it has begun to lay out in recent months, it is imperative that it takes steps to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed.

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. Although these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not yet taking place. Further, it is unclear how the activities of these many organizations interrelate, who should be held accountable for their success

²⁶*Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

²⁷*Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001); *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

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 discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data.

Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important. 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, 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. Routine periodic audits, such as those required in the government information security reforms recently enacted, would allow for more meaningful performance measurement. Agencies and the IGs have completed their first agency reviews and independent evaluations as required by this legislation and submitted their results to OMB. In addition, agencies are also to submit plans of action and milestones for correcting their information security weaknesses. This annual evaluation, reporting, and monitoring process is an important mechanism, previously missing, for holding agencies accountable for implementing effective security and for managing the problem from a governmentwide perspective.

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

OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their computer systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical expertise is 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 that are not supported by a strong agency risk management process.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As the Director of the CERT® Coordination Center testified before this subcommittee last September, “It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.” In addition, in the October 31 advance executive summary of its forthcoming third report, the Gilmore Commission recommended that the President establish a comprehensive plan of research, development, test, and evaluation to enhance cyber security.

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

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