United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Wednesday,
September 23, 1998

INFORMATION SECURITY

Strengthened Management Needed to Protect Critical Federal Operations and Assets

Statement of Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

Mr. Chairman and Members of the Committee:

I am pleased to have this opportunity to provide an assessment of the current state of information security in federal government. Our most recent report, done at the request of this Committee, delineates the serious information security weaknesses placing critical operations and assets at risk and outlines actions needed to further improve security practices across government. The two agencies that you asked us to focus on today—the Department of Veterans Affairs and the Social Security Administration—illustrate the types of risk facing individual departments and agencies as well as actions required to strengthen security management. Recent efforts by these organizations and others throughout government are encouraging because they signify increasing attention to information security concerns, but, as we will discuss today, additional measures are necessary for the federal government to develop and maintain a truly effective security management program.

Information Security Is Drawing Increased Attention

We last provided you an overview of federal information security in September 1996. At that time, serious security weaknesses had been identified at 10 of the largest 15 federal agencies, and we concluded that poor information security was a widespread federal problem.[1] We recommended that the Office of Management and Budget (OMB) play a more active role in overseeing agency practices, in part through its role as chair of the then newly established Chief Information Officers (CIO) Council. Subsequently, in February 1997, as more audit evidence became available, we designated information security as a new governmentwide high-risk area in a series of reports to the Congress.[2]

During 1996 and 1997, federal information security also was addressed by the President's Commission on Critical Infrastructure Protection, which had been established to investigate our nation's vulnerability to both "cyber" and physical threats. In its October 1997 report, Critical Foundations: Protecting America's Infrastructures, the Commission described the potentially devastating implications of poor information security from a national perspective. The report also recognized that the federal government must "lead by example," and included recommendations for improving government systems security. This report eventually led to issuance of Presidential Decision Directive 63 in

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

[2] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

May 1998, which I will discuss in conjunction with other governmentwide security improvement efforts later in my testimony.

Potential Risks Are Increasing

As hearings by this Committee have emphasized, risks to the security of our government's computer systems are significant, and they are growing. The dramatic increase in computer interconnectivity and the popularity of the Internet, while facilitating access to information, are factors that also make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. Further, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are readily available.

Attacks on and misuse of federal computer and telecommunication resources are of increasing concern because these resources are virtually indispensable for carrying out critical operations and protecting sensitive data and assets. For example,

- weaknesses at the Department of the Treasury place over a trillion dollars of annual federal receipts and payments at risk of fraud and large amounts of sensitive taxpayer data at risk of inappropriate disclosure;
- weaknesses at the Health Care Financing Administration place billions of dollars of claim payments at risk of fraud and sensitive medical information at risk of disclosure; and
- weaknesses at the Department of Defense affect operations such as mobilizing reservists, paying soldiers, and managing supplies. Moreover, Defense's warfighting capability is dependent on computer-based telecommunications networks and information systems.

These and other examples of risks to federal operations and assets are detailed in our report Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92), which the Committee is releasing today. Although it is not possible to eliminate these risks, understanding them and implementing an appropriate level of effective controls can reduce the risks significantly. Conversely, an environment of widespread control weaknesses may invite attacks that would otherwise be discouraged.

Serious Weaknesses Continue to Be Identified

As the importance of computer security has increased, so have the rigor and frequency of federal audits in this area. During the last 2 years, we and the agency inspectors general (IG) have evaluated computer-based controls on a wide variety of financial and nonfinancial systems supporting critical federal programs and operations. Many of these audits are now done annually. This growing body of audit evidence is providing a more complete and detailed picture of federal information security than was previously available.

The most recent set of audit results that we evaluated—those published since March 1996—describe significant information security weakness in each of the 24 federal agencies[3] covered by our analysis. These weaknesses cover a variety of areas, which we have grouped into six categories of general control weaknesses.

Access Control Weaknesses

The most widely reported weakness was poor control over access to sensitive data and systems. This area of control was evaluated at 23 of the 24 agencies, and weaknesses were identified at each of the 23. Access control weaknesses make systems vulnerable to damage and misuse by allowing individuals and groups to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them 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 (1) require users to authenticate themselves through the use of secret passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can execute. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to potentially devastating attacks from remote locations all over the world by individuals with minimal computer and telecommunications resources and expertise. Common types of access control weaknesses included

- overly broad access privileges inappropriately provided to very large groups of users;
- access that was not appropriately authorized and documented;

[3] These agencies accounted for 99 percent of reported federal net outlays in fiscal year 1997.

- multiple users sharing the same accounts and passwords, making it impossible to trace specific transactions or modifications to an individual;
- inadequate monitoring of user activity to deter and identify inappropriate actions, investigate suspicious activity, and penalize perpetrators;
- improperly implemented access controls, resulting in unintended access or gaps in access control coverage; and
- access that was not promptly terminated or adjusted when users either left an agency or when their responsibilities no longer required them to have access to certain files.

Service Continuity Weaknesses

The second most widely reported type of weakness pertained to service continuity. Service continuity controls ensure that when unexpected events occur, critical operations continue without undue interruption and critical and sensitive data are protected. In addition to protecting against natural disasters and accidental disruptions, such controls also protect against the growing threat of "cyber-terrorism," where individuals or groups with malicious intent may attack an agency's systems in order to severely disrupt critical operations. 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. 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.

Service continuity controls were evaluated for 20 of the agencies included in our analysis, and weaknesses were reported for all of these agencies. Common weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.
- Disaster recovery plans were not fully tested to identify their weaknesses. One agency's plan was based on an assumption that key personnel could

be contacted within 10 minutes of the emergency, an assumption that had not been tested.

Entitywide Program Planning and Management Weaknesses

The third most common type of weakness involved inadequate entitywide security program planning and 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 cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported.

Weaknesses were reported for all 17 of the agencies for which this area of control was evaluated. Many of these agencies had not developed security plans for major systems based on risk, had not formally documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on.

Segregation of Duties Weaknesses

The fourth most commonly reported type of weakness was inadequate 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.

Segregation of duties is an important internal control concept that applies to both computerized and manual processes.[4] However, it is especially important in computerized environments, since an individual with overly broad access privileges can initiate and execute inappropriate actions, such as software changes or fraudulent transactions, more quickly and with greater impact than is generally possible in a nonautomated environment. 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

[4] Title 2, "Accounting," Appendix II, "Standards for Internal Controls in the Federal Government," GAO Policy and Procedures Manual for Guidance of Federal Agencies.

processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

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 was evaluated at 17 of the 24 agencies. Weaknesses were identified at 16 of these agencies. Common problems involved computer programmers and operators who were authorized to perform a wide variety of duties, thus enabling them to independently modify, circumvent, and disable system security features. For example, at one agency, all users of the financial management system could independently perform all of the steps needed to initiate and complete a payment—obligate funds, record vouchers for payment, and record checks for payment—making it relatively easy to make a fraudulent payment.

Application Software Development and Change Control Weaknesses

The fifth most commonly reported type of weakness pertained to software development and change controls. Such controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects 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 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 14 of the 18 agencies where such controls were evaluated. One of the most common types of weakness in this area was undisciplined testing procedures that did not ensure that implemented software operated as intended. In addition, 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.

System Software Control Weaknesses

The sixth area pertained to operating system software controls. 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 programs 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 disclosures. 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.

A common type of system software control weakness reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a wide variety of ways. For example, at one facility, 88 individuals had the ability to implement programs not controlled by the security software, and 103 had the ability to access an unencrypted security file containing passwords for authorized users.

Significant system software control weaknesses were reported at 9 of the 24 agencies. In the remaining 15 agencies, this area of control had not been fully evaluated. We are working with the IGs to ensure that it receives adequate coverage in future evaluations.

I would now like to describe in greater detail weaknesses at the two agencies that you have chosen to feature today: the Department of Veterans Affairs and the Social Security Administration.

Weaknesses at the Department of Veterans Affairs

The Department of Veterans Affairs (VA) relies on a vast array of computer systems and telecommunications networks to support its operations and store the sensitive information the department collects in carrying out its mission. In a report released today, we identify general computer control weaknesses that place critical VA operations, such as financial management, health care delivery, benefit payments, life insurance services, and home mortgage loan guarantees, at risk of misuse and disruption.[5] In addition, sensitive information contained in VA's systems, including financial transaction data and personal information on veteran medical records and benefit payments, is vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction—possibly occurring without detection.

VA operates the largest health care delivery system in the United States and guarantees loans on about 20 percent of the homes in the country. In fiscal year 1997, VA spent over $17 billion on medical care and processed over 40 million benefit payments totaling over $20 billion. The department also provided insurance protection through more than 2.5 million policies that represented about $24 billion in coverage at the end of fiscal year 1997. In addition, the VA systems support the department's centralized accounting and payroll functions. In fiscal year 1997, VA's payroll was almost $11 billion, and the centralized accounting system generated over $7 billion in additional payments.

In our report, we note significant problems related to the department's control and oversight of access to its systems. VA did not adequately limit

[5] VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

the access of authorized users or effectively manage user identifications (ID) and passwords.

- At one facility, the security software was implemented in a manner that provided all of the more than 13,000 users with the ability to access and change sensitive data files, read system audit information, and execute powerful system utilities. Such broad access authority increased the risk that users could circumvent the security software to alter payroll and other payment transactions. This weakness could also provide users the opportunity to access and disclose sensitive information on veteran medical records, such as diagnoses, procedures performed, inpatient admission and discharge data, or the purpose of outpatient visits, and home mortgage loans, including the purpose, loan balance, default status, foreclosure status, and amount delinquent.
- At two facilities, we found that system programmers had access to both system software and financial data. This type of access could allow the programmers to make unauthorized changes to benefit payment information without being detected.
- At four of the five facilities we visited, we identified user ID and password management control weaknesses that increased the risk of passwords being compromised to gain unauthorized access. For example, IDs for terminated or transferred employees were not being disabled, many passwords were common words that could be easily guessed, numerous staff were sharing passwords, and some user accounts did not have passwords These types of weaknesses make the financial transaction data and personal information on veteran medical records and benefits stored on these systems vulnerable to misuse, improper disclosure, and destruction. We demonstrated these vulnerabilities by gaining unauthorized access to VA systems and obtaining information that could have been used to develop a strategy to alter or disclose sensitive patient information.

We also found that the department had not adequately protected its systems from unauthorized access from remote locations or through the VA network. The risks created by these issues are serious because, in VA's interconnected environment, the failure to control access to any system connected to the network also exposes other systems and applications on the network.

- While simulating an outside hacker, we gained unauthorized access to the VA network. Having obtained this access, we were able to identify other systems on the network, which makes it much easier for outsiders with no knowledge of VA's operations or infrastructure to penetrate the department's computer resources. We used this information to access the log-on screen of another computer that contained financial and payroll data, veteran loan information, and sensitive information on veteran medical records for both inpatient and outpatient treatment. Such access to the VA network, when coupled with VA's ineffective user ID and password management controls and available "hacker" tools, creates a significant risk that outside hackers could gain unauthorized access to this information.

- At two facilities, we were able to demonstrate that network controls did not prevent unauthorized users with access to VA facilities or authorized users with malicious intent from gaining improper access to VA systems. We were able to gain access to both mainframe and network systems that could have allowed us to improperly modify payments related to VA's loan guaranty program and alter sensitive veteran compensation, pension, and life insurance benefit information. We were also in a position to read and modify sensitive data.

The risks created by these access control problems were also heightened significantly because VA was not adequately monitoring its systems for unusual or suspicious access activities. In addition, the department was not providing adequate physical security for its computer facilities, assigning duties in such a way as to properly segregate functions, controlling changes to powerful operating system software, or updating and testing disaster recovery plans to ensure that the department could maintain or regain critical functions in emergencies.

Many similar access and other general computer control weaknesses had been reported in previous years, indicating that VA's past actions have not been effective on a departmentwide basis. Weaknesses associated with restricting access to sensitive data and programs and monitoring access activity have been consistently reported in IG and other internal reports.

A primary reason for VA's continuing general computer control problems is that the department does not have a comprehensive computer security planning and management program in place to ensure that effective controls are established and maintained and that computer security receives adequate attention. An effective program would include guidance and procedures for assessing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls. However, VA had not clearly delineated security roles and responsibilities; performed regular, periodic assessments of risk; implemented security policies and procedures that addressed all aspects of VA's interconnected environment; established an ongoing monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; or instituted a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

In our report to VA, we recommended that the Secretary direct the CIO to (1) work with the other VA CIOs to address all identified computer control weaknesses, (2) develop and implement a comprehensive departmentwide computer security planning and management program, (3) review and assess computer control weaknesses identified throughout the department and establish a process to ensure that these weaknesses are addressed, and (4) monitor and periodically report on the status of improvements to computer security throughout the department.

In commenting on our report, VA agreed with these recommendations and stated that the department would immediately correct the identified computer control weaknesses and implement oversight mechanisms to ensure that these problems do not reoccur. VA also stated that the department was developing plans to correct deficiencies previously identified by the IG and by internal evaluations and that the VA CIO will report periodically on VA's progress in correcting computer control weaknesses throughout the department. We have discussed these actions with VA officials, and, as part of our upcoming review, we will be examining completed actions and evaluating their effectiveness.

Weaknesses at the Social Security Administration

The Social Security Administration (SSA) relies on extensive information processing resources to carry out its operations, which, for 1997, included payments that totaled approximately $390 billion to 50 million beneficiaries. This was almost 25 percent of the $1.6 trillion in that year's federal expenditures. SSA also issues social security numbers and maintains earnings records and other personal information on virtually all U. S. citizens. Through its programs, SSA processes approximately 225 million wage and tax statements (W-2 forms) annually for approximately 138 million workers. Few federal agencies affect so many people.

The public depends on SSA to protect trust fund revenues and assets from fraud and to protect sensitive information on individuals from inappropriate disclosure. In addition, many current beneficiaries rely on the uninterrupted flow of monthly payments to meet their basic needs. In

November 1997, the SSA IG reported serious weaknesses in controls over information resources, including access, continuity of service, and software program changes that unnecessarily place these assets and operations at risk.[6] These weaknesses demonstrate the need for SSA to do more to assure that adequate controls are provided for information collected, processed, transmitted, stored, or disseminated in general support systems or major applications.

Internal control testing identified information protection-related weaknesses throughout SSA's information systems environment. Affected areas included SSA's distributed computer systems as well as its mainframe computers. These vulnerabilities exposed SSA and its computer systems to external and internal intrusion; subjected sensitive SSA information related to social security numbers, earnings, disabilities, and benefits to potential unauthorized access, modification, and/or disclosure; and increased the risks of fraud, waste, and abuse. Access control and other weaknesses also increased the risks of introducing errors or irregularities into data processing operations.

For example, auditors identified numerous employee user accounts on SSA networks, including dial-in modems, that were either not password protected or were protected by easily guessed passwords. These weaknesses increased the risk that unauthorized outsiders could access, modify, and delete data; create, modify, and delete users; and disrupt services on portions of SSA's network. In addition, auditors identified network control weaknesses that could result in accidental or intentional alteration of birth and death records, as well as unauthorized disclosure of personal data and social security numbers.

These weaknesses were made worse because security awareness among employees was not consistent at SSA. As a result, SSA was susceptible to security penetration techniques, such as social engineering, whereby users disclose sensitive information in response to seemingly legitimate requests from strangers either over the phone or in person. The auditors reported that during testing, they were able to secure enough information through social engineering to allow access to SSA's network.

Further, by applying intrusion techniques in penetration tests, auditors gained access to various SSA systems that would have allowed them to view user data, add and delete users, modify network configurations, and disrupt service to users. By gaining access through such tests, auditors

[6] Social Security Accountability Report for Fiscal Year 1997, SSA Pub. No. 31-231, November 1997.

also were able to execute software tools that resulted in their gaining access to SSA electronic mailboxes, public mailing lists, and bulletin boards. This access would have provided an intruder the ability to read, send, or change e-mail exchanged among SSA users, including messages from or to the Commissioner.

In addition to access control weaknesses and inadequate user awareness, employee duties at SSA were not appropriately segregated to reduce the risk that an individual employee could introduce and execute unauthorized transactions without detection. As a result, certain employees had the ability to independently carry out actions such as initiating and adjudicating claims or moving and reinstating earnings data. This weakness was exacerbated because certain mitigating monitoring or detective controls could not be relied on. For example, SSA has developed a system that allows supervisors to review sensitive or potentially fraudulent activity. However, key transactions or combinations of transactions are not being reviewed or followed up promptly and certain audit trail features have not been activated.

Weaknesses such as those I have just described increase the risk that a knowledgeable individual or group could fraudulently obtain payments by creating fictitious beneficiaries or increasing payment amounts. Similarly, such individuals could secretly obtain sensitive information and sell or otherwise use it for personal gain.

The recent growth in "identity theft," where personal information is stolen and used fraudulently by impersonators for purposes such as obtaining and using credit cards, has created a market for such information. According to the SSA IG's September 30, 1997, report to the Congress (included in the SSA's fiscal year 1997 Accountability Report), 29 criminal convictions involving SSA employees were obtained during fiscal year 1997, most of which involved creating fictitious identities, fraudulently selling SSA cards, misappropriating refunds, or abusing access to confidential information. The risk of abuse by SSA employees is of special concern because, except for a very few individuals, SSA does not restrict access to view sensitive data based on a need-to-know basis. As a result, a large number of SSA employees can browse enumeration, earnings, and claims records for many other individuals, including other SSA employees, without detection. SSA provides this broad access because it believes that doing so facilitates its employees' ability to carry out SSA's mission.

An underlying factor that contributes to SSA's information security weaknesses is inadequate entitywide security program planning and management. Although SSA has an entitywide security program in place, it does not sufficiently address all areas of security, including dial-in access, telecommunications, certain major mainframe system applications, and distributed systems outside the mainframe environment. A lack of such an entitywide program impairs each group's ability to develop a security structure for its responsible area and makes it difficult for SSA management to monitor agency performance in this area.

In two separate letters to SSA management, the IG and its contractor made recommendations to address the weaknesses reported in November 1997. SSA has agreed with the majority of the recommendations and is developing related corrective action plans.

Improvements Require Individual Agency Actions and Strengthened Central Oversight

Substantively improving federal information security will require efforts at both the individual agency level and at the governmentwide level. Agency managers are primarily responsible for securing the information resources that support their critical operations. However, central oversight also is important to monitor agency performance and address crosscutting issues that affect multiple agencies. Over the last 2 years, a number of efforts have been initiated, but additional actions are still needed.

Improved Security Program Management Needed at Individual Agencies

First, it is important that agency managers implement comprehensive programs for identifying and managing their security risks in addition to correcting specific reported weaknesses. Over the last 2 years, our reports and IG reports have included scores of recommendations to individual agencies, and agencies have either implemented or planned actions to address most of the specific weaknesses. However, there has been a tendency to react to individual audit findings as they were reported, with little ongoing attention to the systemic causes of control weaknesses.

In short, agencies need to move beyond addressing individual audit findings and supplement these efforts with a framework for proactively managing the information security risks associated with their operations. Such a framework includes determining which risks are significant, assigning responsibility for taking steps to reduce risks, and ensuring that these steps are implemented effectively and remain effective over time. Without a management framework for carrying out these activities, information security risks to critical operations may be poorly understood;

responsibilities may be unclear and improperly implemented; and policies and controls may be inadequate, ineffective, or inconsistently applied.

Best Practices of Leading Organizations Provide Guidance

In late 1996, at the Committee's request, we undertook an effort to identify potential solutions to this problem, including examples that could supplement existing guidance to agencies. To do this, we studied the security management practices of eight nonfederal organizations known for their superior security programs. These organizations included two financial services corporations, a regional electric utility, a state university, a retailer, a state agency, a computer vendor, and an equipment manufacturer.

We found that these organizations managed their information security risks through a cycle of risk management activities, and we identified 16 specific practices that supported these risk management principles. These practices are outlined in an executive guide titled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), which was released by the Committee in May 1998 and endorsed by the CIO Council. Upon publication, the guide was distributed to all major agency heads, CIOs, and IGs.

The guide describes a framework for managing information security risks through an ongoing cycle of activities coordinated by a central focal point. Such a framework can help ensure that existing controls are effective and that new, more advanced control techniques are prudently and effectively selected and implemented as they become available. The risk management cycle and the 16 practices supporting this cycle of activity are depicted in the following figures.

Figure 1: The Risk Management Cycle

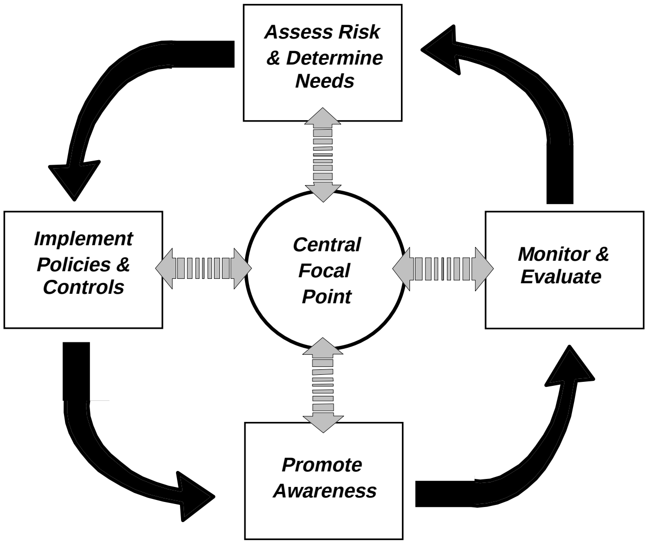
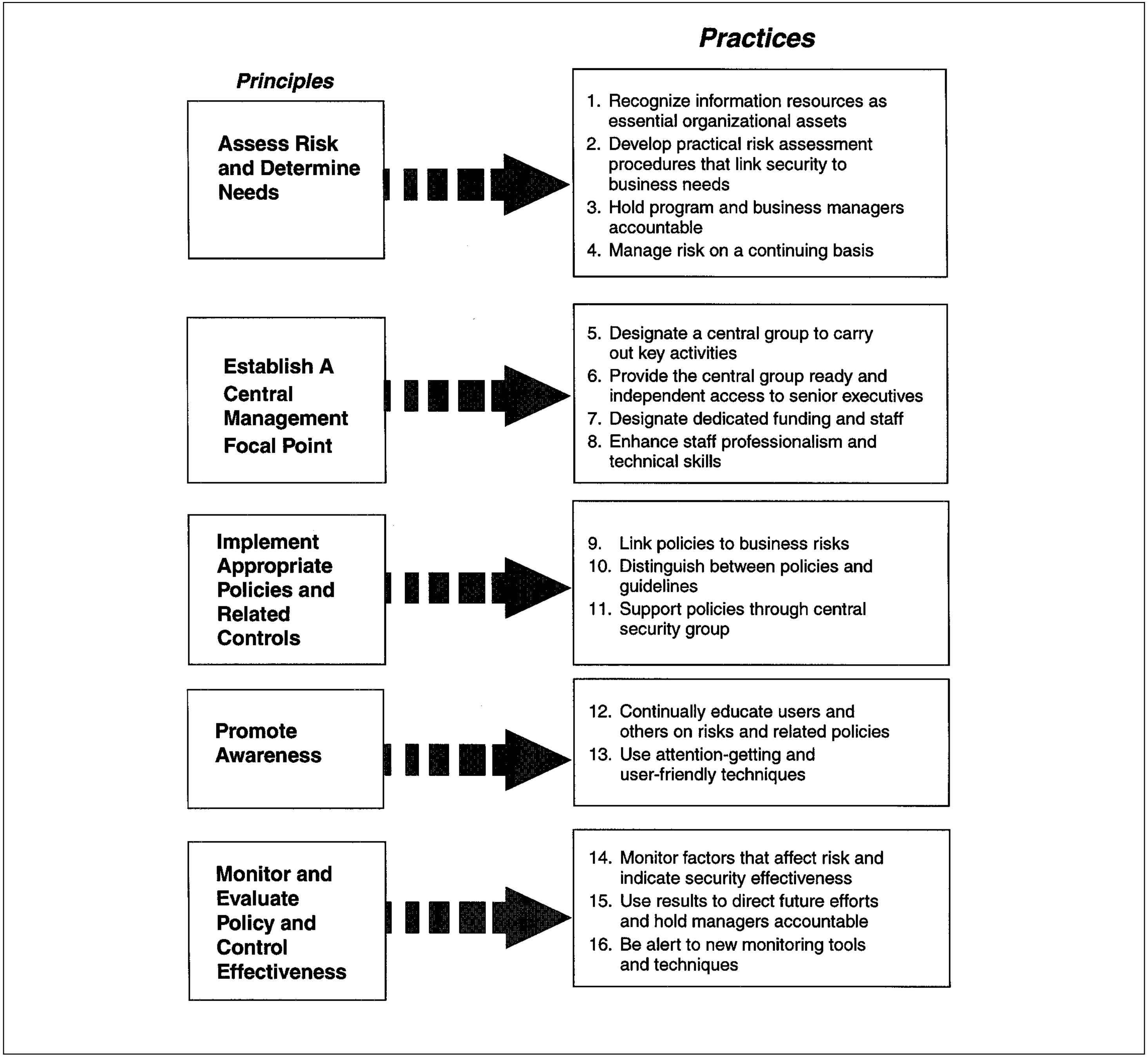


Figure 2: Sixteen Practices Employed by Leading Organizations to Implement the Risk Management Cycle



Principles

Practices

Assess Risk and Determine Needs

1. Recognize information resources as essential organizational assets
2. Develop practical risk assessment procedures that link security to business needs
3. Hold program and business managers accountable
4. Manage risk on a continuing basis

Establish A Central Management Focal Point

5. Designate a central group to carry out key activities
6. Provide the central group ready and independent access to senior executives
7. Designate dedicated funding and staff
8. Enhance staff professionalism and technical skills

Implement Appropriate Policies and Related Controls

9. Link policies to business risks
10. Distinguish between policies and guidelines
11. Support policies through central security group

Promote Awareness

12. Continually educate users and others on risks and related policies
13. Use attention-getting and user-friendly techniques

Monitor and Evaluate Policy and Control Effectiveness

14. Monitor factors that affect risk and indicate security effectiveness
15. Use results to direct future efforts and hold managers accountable
16. Be alert to new monitoring tools and techniques

Centrally Directed Improvement Efforts Have Increased

In addition to effective security program planning and management at individual agencies, governmentwide leadership, coordination, and oversight are important to

- ensure that federal executives understand the risks to their operations,
- monitor agency performance in mitigating these risks,
- ensure implementation of needed improvements, and
- facilitate actions to resolve issues affecting multiple agencies.

To help achieve this, the Paperwork Reduction Act of 1980 made OMB responsible for developing information security policies and overseeing related agency practices. In 1996, we reported that OMB's oversight consisted largely of reviewing selected agency system-related projects and participating in various federal task forces and working groups. While these activities are important, we recommended that OMB play a more active role in overseeing agency performance in the area of information security.

Since then, OMB's efforts have been supplemented by those of the CIO Council. In late 1997, the Council, under OMB's leadership, designated information security as one of six priority areas and established a Security Committee, an action that we had recommended in 1996. The Security Committee, in turn, has established relationships with other federal entities involved in security and developed a very preliminary plan. While the plan does not yet comprehensively address the various issues affecting federal information security or provide a long-range strategy for improvement, it does cover important areas by specifying three general objectives: promote awareness and training, identify best practices, and address technology and resource issues. During the first half of 1998, the committee has sponsored a security awareness seminar for federal agency officials and developed plans for improving agency access to incident response services.

More recently, in May 1998, Presidential Decision Directive (PDD) 63 was issued in response to recommendations made by the President's Commission on Critical Infrastructure Protection in October 1997.[7] PDD 63 established entities within the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation to address critical infrastructure protection, including federal agency information infrastructures. Specifically, the directive states that "the Federal

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

Government shall serve as a model to the private sector on how infrastructure assurance is best achieved" and that federal department and agency CIOs shall be responsible for information assurance. The directive requires each department and agency to develop a plan within 180 days from the issuance of the directive in May 1998 for protecting its own critical infrastructure, including its cyber-based systems. These plans are then to be subject to an expert review process. Other key provisions related to the security of federal information systems include

- a review of existing federal, state, and local bodies charged with information assurance tasks;
- enhanced collection and analysis of information on the foreign information warfare threat to our critical infrastructures;
- establishment of a National Infrastructure Protection Center within the Federal Bureau of Investigation to facilitate and coordinate the federal government's investigation and response to attacks on its critical infrastructures;
- assessments of U. S. government systems' susceptibility to interception and exploitation; and
- incorporation of agency infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

We plan to follow up on the these activities as more specific information becomes available.

A Comprehensive and Coordinated Governmentwide Strategy Needs to Emerge

The CIO Council's efforts and the issuance of PDD 63 indicate that senior federal officials are increasingly concerned about information security risks and are acting on these concerns. Improvements are needed both at the individual agency level and in central oversight, and coordinated actions throughout the federal community will be needed to substantively improve federal information security.

What needs to emerge is a coordinated and comprehensive strategy that incorporates the worthwhile efforts already underway and takes advantage of the expanded amount of evidence that has become available in recent years. The objectives of such a strategy should be to encourage agency improvement efforts and measure their effectiveness through an appropriate level of oversight. This will require a more structured approach for (1) ensuring that risks are fully understood, (2) promoting use of the most cost-effective control techniques, (3) testing and evaluating the effectiveness of agency programs, and (4) acting to address identified deficiencies. This approach needs to be applied at individual departments and agencies and in a coordinated fashion across government.

In our report on governmentwide information security that is being released today, we recommended that the Director of OMB and the Assistant to the President for National Security Affairs develop such a strategy. As part of our recommendation, we stated that such a strategy should

- ensure that executive agencies are carrying out the responsibilities outlined in laws and regulations requiring them to protect the security of their information resources;
- clearly delineate the roles of the various federal organizations with responsibilities related to information security;
- identify and rank the most significant information security issues facing federal agencies;
- promote information security risk awareness among senior agency officials whose critical operations rely on automated systems;
- identify and promote proven security tools, techniques, and management best practices;
- ensure the adequacy of information technology workforce skills;
- ensure that the security of both financial and nonfinancial systems is adequately evaluated on a regular basis;
- include long-term goals and objectives, including time frames, priorities, and annual performance goals; and
- provide for periodically evaluating agency performance from a governmentwide perspective and acting to address shortfalls.

In commenting on a draft of our report, the OMB's Acting Deputy Director for Management said that a plan is currently being developed by OMB and the CIO Council, working with the National Security Council. The comments stated that the plan is to develop and promote a process by which government agencies can (1) identify and assess their existing security posture, (2) implement security best practices, and (3) set in motion a process of continued maintenance. The comments also describe plans for a CIO Council-sponsored interagency assist team that will review agency security programs. As of September 17, a plan had not yet been finalized and, therefore, was not available for our review, according to an OMB official involved in the plan's development. We intend to review the plan as soon as it is available.

Year 2000 Crisis Increases Sense of Urgency for Improved Security

Although information security, like other types of safeguards and controls, is an ongoing concern, it is especially important, now and in the coming 18 months, as we approach and deal with the computer problems associated with the Year 2000 computing crisis. The Year 2000 crisis presents a number of security problems with which agencies must be prepared to contend.

For example, it is essential that agencies improve the effectiveness of controls over their software development and change process as they implement the modifications needed to make their systems Year 2000 compliant. Many agencies have significant weaknesses in this area, and most are under severe time constraints to make needed software changes. As a result, there is a danger that already weak controls will be further diminished if agencies bypass or truncate them in an effort to speed the software modification process. This increases the risk that erroneous or malicious code will be implemented or that systems that do not adequately support agency needs will be rushed into use.

Also, agencies should strive to improve their abilities to detect and respond to anomalies in system operations that may indicate unauthorized intrusions, sabotage, misuse, or damage that could affect critical operations and assets. As illustrated by VA and SSA, many agencies are not taking full advantage of the system and network monitoring tools that they already have and many have not developed reliable procedures for responding to problems once they are identified. Without such incident detection and response capabilities, agencies may not be able to readily distinguish between malicious attacks and system-induced problems, such as those stemming from Year 2000 noncompliance, and respond appropriately.

The Year 2000 crisis is the most dramatic example yet of why we need to protect critical computer systems because it illustrates the government's widespread dependence on these systems and the vulnerability to their disruption. However, the threat of disruption will not end with the advent of the new millennium. There is a longer-term danger of attack from malicious individuals or groups, and it is important that our government design long-term solutions to this and other security risks.

Mr. Chairman, this concludes our statement. We would be happy to respond to any questions you or other members of the Committee may have.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO’s World Wide Web Home Page at:

http://www.gao.gov