United States General Accounting Office

GAO

Testimony

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

For Release on
Tuesday,
May 19, 1998

INFORMATION SECURITY

Serious Weaknesses Put State Department and FAA Operations at Risk

Statement for the Record by Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

GAO/T-AIMD-98-170

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 19051998	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) GAO	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 20	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5/19/98	Report

4. TITLE AND SUBTITLE
Information Security - Serious Weaknesses Put State Department and FAA Operations at Risk

5. FUNDING NUMBERS

6. AUTHOR(S)
Gene Dodaro

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This testimony focuses on the results of recent reviews of the Department of State and the Federal Aviation administration (FAA). Significant computer security weaknesses at both these organizations threaten the integrity of their operations, numerous specific recommendations for improving State and FAA's information security posture have been made. Unfortunately, such weaknesses are typical at most federal agencies evaluated. However, good management practices and organizational discipline can do much to mitigate the risks all government agencies face from security threats. Accordingly, also highlighted are best practices identified in studying leading organizations that can be used by all agencies to protect sensitive information and computer systems.

14. SUBJECT TERMS
Information, Security

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Mr. Chairman and Members of the Committee:

We are pleased to be asked to discuss our work in computer security. As requested, our testimony will focus on the results of our recent reviews of the Department of State and the Federal Aviation Administration (FAA). Significant computer security weaknesses at both these organizations threaten the integrity of their operations, and we have made numerous specific recommendations for improving State and FAA's information security posture. Unfortunately, such weaknesses are typical at most federal agencies we evaluate. However, good management practices and organizational discipline can do much to mitigate the risks all government agencies face from security threats. Accordingly, we will also highlight best practices we have identified in studying leading organizations that can be used by all agencies to protect sensitive information and computer systems.

Computer Security Is an Increasing Threat to Critical Government Operations

The dramatic increase in computer interconnectivity and the popularity of the Internet are offering government agencies unprecedented opportunities to improve operations by reducing paper processing, cutting costs, and sharing information. At the same time, however, malicious attacks on computer systems are increasing at alarming rates and are posing serious risks to key government operations. Thus, the ultimate success of agencies' ability to use interconnected systems to carry out critical governmental functions depends in large part on their ability to protect the integrity, privacy, and availability of the data and systems they rely upon.

This Committee has long been concerned about the need to protect sensitive information in federal computer systems. These concerns are well-founded. At the request of you, Mr. Chairman, and Senator Glenn, we have undertaken a large body of work to address the issue, including reviews of most of the federal government's largest departments' and agencies' computer security programs. In conjunction with our financial statement audit focus and high-risk reviews, this work has revealed a disturbing picture of our government's lack of success in protecting federal assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption. For example:

- In May 1996, we reported that computer hackers had penetrated Department of Defense computer systems; obtained and corrupted

sensitive information; shut down and crashed entire systems and networks; and denied service to users who depend on automated systems to help meet critical missions, including weapons and supercomputer research, logistics, procurement, and military health. Our recommendations focused on the need for Defense to assign clear responsibility and accountability for the successful implementation of its security program, improve its security policies and procedures, increase security awareness, and implement more proactive technical protection and monitoring systems.[1]

- In September 1996, we reported that, over the previous 2 years, serious weaknesses had been reported for 10 of the largest federal agencies, concluding that poor information security was a widespread federal problem with potentially devastating consequences.[2] In that report, we recommended that the Office of Management and Budget (OMB) play a more proactive role in overseeing agency practices and managing improvements, in part through its role as chair of the Chief Information Officers (CIO) Council.
- In February 1997, we identified information security across all government agencies as a high-risk area. We found management and system controls to be largely inadequate, leaving critical operations at many agencies highly vulnerable to unauthorized access.[3]
- In three 1997 reports, we identified a wide range of continuing serious weaknesses in Internal Revenue Service (IRS) systems, including inadequate controls over employee browsing of taxpayer records.[4]
- In March 1998, in our report on the federal government's consolidated financial statements, we emphasized that pervasive computer control weaknesses were placing enormous amounts of federal assets at risk of fraud and misuse, financial information at risk of inappropriate disclosure, and critical operations at risk of disruption.[5]

[1]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

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

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

[4]IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997); Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-89, August 29, 1997); and Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997).

[5]Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998).

Also at your request, we are currently (1) examining computer security programs at other selected agencies including the National Aeronautics and Space Administration, (2) developing a comprehensive and detailed analysis of information security problems at the largest federal agencies, and (3) producing an updated summary of actions taken by OMB and the CIO Council to address these problems from a governmentwide perspective.

Today, the Committee is releasing the redacted versions of our reports on computer security at State and FAA.[6] These reviews resulted in many findings that are too sensitive to discuss in today's open setting and, accordingly, detailed reports have been provided to this Committee and to appropriate agency officials under separate covers. However, we will describe the types of weaknesses found and the risks they posed to critical systems and information.

Pervasive Computer Security Weaknesses Threaten State Department Operations

Last year, this Committee asked us to assess whether the State Department's unclassified automated information systems were susceptible to unauthorized access. State relies on a variety of decentralized information systems and networks to help it carry out its responsibilities and support business functions, such as personnel, financial management, medical, visas, passports, and diplomatic agreements and communications. The data stored in these systems, although unclassified, are sensitive enough to be attractive targets for individuals and organizations seeking monetary gain or desiring to learn about or damage State operations. For example, much of this information deals with employees working for the department and includes American and Foreign Service National personnel records, employee and retiree data, and private health records. Background investigation information about employees being considered for security clearances is also processed on State's unclassified network.

The potential consequences of misuse of this information are of major concern. For example, unauthorized deletion or alteration of data could enable known criminals, terrorists, and other dangerous individuals to enter the United States. Personnel information concerning approximately 35,000 State employees could be useful to foreign governments wishing to build personality profiles on selected employees. Manipulation of financial

[6]Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998) and Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

data could result in overpayments or underpayments to vendors, banks, and individuals, and inaccurate information being provided to agency managers and the Congress. Furthermore, the overseas activities of other federal agencies may be jeopardized to the extent they are supported by State systems.

To determine State's vulnerability to computer attacks, we tested the department's technical and physical controls for ensuring that data, systems, and facilities are protected from unauthorized access. We designed our tests to simulate two security penetration scenarios: (1) an unauthorized individual who has no knowledge of State's automated information infrastructure (for example, a hacker or terrorist organization) and (2) a mid-level internal user with limited access privileges and some specific computer related information (for example, a State employee) exceeding his or her limited privileges.

In simulating these scenarios, we wanted to know whether an unauthorized user could compromise—that is, improperly access, modify, disclose, or destroy—sensitive data if he or she successfully penetrated State's computer resources. During our testing, we performed controlled penetration attacks at dial-in access points, internal network security controls, the department's Internet gateways, and public information servers. We also attempted to gain unauthorized physical access to certain State facilities and assessed users' awareness by attempting to get them to reveal sensitive information, such as their passwords. Such techniques, sometimes referred to as social engineering, can be used by attackers to easily bypass an organization's existing physical and logical security controls.

Unfortunately, our penetration tests were largely successful. They demonstrated that State's computer systems and the information contained within them are very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses. For example, without any passwords or specific knowledge of State's systems, we successfully gained access to State's networks through dial-in connections to modems. Having obtained this access, we could have modified, stolen, downloaded, or deleted important data; shut down services; and monitored network traffic, such as e-mail and data files.

In addition, by posing as a trusted inside computer user, we were able to circumvent State's internal network security controls and access information and sensitive data that would normally be off limits to most employees. For example, after we gained (administrator) access[7] to host systems on several different operating platforms, such as UNIX and Windows NT, we viewed international financial information, travel arrangements, detailed network diagrams, a listing of valid users on local area networks, employees' e-mail, performance appraisals, and other sensitive data.

Our tests also showed that security awareness among State employees was problematic. For example, many computer users at State had weak passwords that were easily guessed, indicating that they were unaware of, or insensitive to, the need for secure passwords. One way to prevent password guessing is to ensure that users choose complex passwords, such as those composed of alphanumeric, upper- and lower-case characters. However, we found no evidence that State was training its users to employ these techniques. We also found little evidence that State was training its users to refrain from disclosing sensitive information. For example, we called a user under the pretense that we were systems maintenance personnel and were able to convince her to disclose her password.

We also obtained access to State's networks by breaching physical security at one facility, and finding user account information and active terminal sessions in unattended areas. For example, in several instances we were able to enter a State facility without required identification. In an unlocked office, we found unattended personal computers logged onto a local area network. We also found a user identification and password taped to one of the computers. Using these terminals, we were able to download a file that contained a password list. This list could have been used later to help hack into State's systems. In another unlocked area, we were able to access the local area network server and obtain supervisor-level access to a workstation, which would have allowed us to even more easily circumvent controls and hide any traces of our activities.

Internet security was the only area in which we found that State's controls were currently adequate. We attempted to gain access to internal State networks by going through and around State's Internet gateways or

[7]Also known as "superuser" access, obtaining this access level permits total control of a system's operations and security functions. With system administrator rights, one can start up and shut down a system; add and remove system users; install or delete system software; and read, modify, or delete all system data.

exploiting information servers from the outside via the Internet, but we were not able to gain access to State's systems. State's protection in this area was adequate, in part, because the department currently limits use and access to the Internet. However, State officials have been requesting greater Internet access and the department is considering various options for providing it.

Expansion of Internet services would provide more pathways and additional tools for an intruder to attempt to enter unclassified computer resources and therefore increase the risk to State systems. Recognizing this, State conducted an analysis of the risks involved with increasing Internet use. However, the department has not yet decided to what extent it will accept and/or address these new risks. Until it does so, State will not be in a good position to expand its Internet use.

The primary reason why our penetration tests were successful is that State, like many federal agencies, lacks the basic building blocks necessary to effectively manage information security risks. First, State did not have a central focal point to oversee and coordinate security activities. Computer security responsibilities were fragmented among three organizations—the Chief Information Office, Diplomatic Security, and Information Management—none of which had the authority to effect necessary changes. Second, State did not routinely perform risk assessments so that its sensitive information could be protected based on its sensitivity and criticality to mission-related operations. Third, the department's primary information security policy document was incomplete. Fourth, State was not adequately ensuring that computer users were fully aware of the risks and responsibilities of protecting sensitive information. Fifth, the department did not routinely monitor and evaluate the effectiveness of its security programs, and it did not established a robust incident response capability.

A key reason why these critical elements of security were not in place was that top managers at State had not demonstrated a commitment to establishing a comprehensive and effective information security program. For example, even though State had reported mainframe computer security to the President and the Congress as a material weakness under the Federal Managers' Financial Integrity Act for the past 10 years,[8] the problem had not yet been corrected. In addition, information security had often been assigned to low- and mid-level State employees as a collateral

[8]The Federal Managers' Financial Integrity Act: 1996 Report to the President and the Congress (United States Department of State, December 1996).

duty. Finally, State's top managers had still not developed a comprehensive security plan or ensured that appropriate resources were devoted to improving computer security.

In our report being released today, we recommended that State take a number of actions to address these weaknesses to improve its information security posture. For example, we recommended that the Secretary of State

- establish a central information security unit with responsibility for facilitating, coordinating, and overseeing departmental information security activities;
- develop and maintain an up-to-date security plan;
- develop policies and procedures that require senior State managers to evaluate the risks to their sensitive information and systems and determine appropriate solutions;
- assign the CIO the responsibility and full authority for ensuring that the information security policies, procedures, and practices of the agency are adequate; and
- defer expansion of Internet usage until State addresses known vulnerabilities and provides appropriate security measures commensurate with risks associated with the planned level of Internet expansion.

In addition, we provided State with dozens of suggested solutions to mitigate the specific weaknesses that our tests identified.

We are pleased to report that in concurring with our recommendations, State identified a number of actions it is beginning to take to strengthen its information security program. For example, State advised us that its Chief Information Officer is beginning to address the lack of a central focus for information systems security by establishing a Security Infrastructure Working Group. State also agreed to formalize and document risk management decisions, revise provisions of the Foreign Affairs Manual related to information security, and undertake an evaluation of one of its most significant networks based on our review. Furthermore, State said it is implementing a plan to correct the technical weaknesses identified during our testing. However, State did not agree with our recommendation to defer expansion of Internet use until the department addresses known vulnerabilities. In explaining its nonconcurrence, State asserted that expanding Internet usage is a priority and that the department has a plan to mitigate the risks of expansion.

FAA's Weak Computer Security Practices Jeopardize Flight Safety

Given the paramount need to ensure safe air travel, this Committee also asked us to review FAA's computer security program. FAA's air traffic control (ATC) computer systems provide information to air traffic controllers and aircraft flight crews to ensure safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruptions of air traffic or even loss of life due to collisions.

To determine whether computer security at FAA is effective, we were asked to assess (1) whether FAA was effectively managing physical security at ATC facilities, (2) whether FAA was effectively managing systems security for its current operational systems, (3) whether FAA was effectively managing systems security for future ATC modernization systems, and (4) the effectiveness of its management structure and implementation of policy for computer security. We elected not to perform penetration testing at FAA because, in the early phases of our work, we already had (1) identified serious deficiencies in each of the areas we reviewed, (2) found evidence of ATC systems that had been penetrated and critical ATC data compromised, and (3) determined that FAA had planned to conduct its own penetration tests on select ATC systems.

We found that FAA was not effectively managing physical security at ATC facilities. Known weaknesses exist at many facilities. For example, at one facility, an FAA inspection report disclosed that service contract employees were given unrestricted access to sensitive areas without having appropriate background investigations. FAA's assessment of another facility that controls aircraft concluded that access control procedures were weak to nonexistent and that the facility was extremely vulnerable to criminal and terrorist attacks. Furthermore, we found that FAA did not know if other facilities were similarly vulnerable because it had not assessed the physical security controls at 187 facilities since 1993.

FAA also was ineffective in managing systems security for its operational systems and was in violation of its own policy. A review conducted for FAA's Office of Civil Aviation Security in October 1996 by the Volpe National Transportation Systems Center[9] concluded that FAA had performed the necessary analysis to determine system threats, vulnerabilities, and safeguards for only 3 of 90 operational ATC computer

[9]The John A. Volpe National Transportation Systems Center, located in Cambridge, Massachusetts, is a federal government organization whose principal role is to serve as a national center for transportation and logistics expertise. It provides research, management, and engineering support to the U.S. Department of Transportation, other federal agencies, and state and local governments.

systems, or less than 4 percent.[10] FAA officials told us that this was an accurate depiction of the current state of operational systems security. In addition, only one of the nine operational ATC telecommunications networks had been analyzed. Such poor security management existed despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety." FAA's 1997 Telecommunications Strategic Plan continued to identify security of telecommunication systems as an area in need of improvement. Without knowing the specific vulnerabilities of its ATC systems, FAA cannot adequately protect them.

FAA claimed that because current ATC systems often utilize custom-built, 20-year-old equipment with special purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. While these configurations may not be commonly understood by external hackers, one cannot assume that old or obscure systems are, a priori, secure. In addition, the certification reports that FAA has done revealed operational systems vulnerabilities. Furthermore, archaic and proprietary features of the ATC system provide no protection from attack by disgruntled current and former employees who understand them.

Additionally, FAA had not been effectively managing systems security for future ATC modernization systems. FAA had no security architecture, security concept of operations, or security standards. As a result, implementation of security requirements across ATC development efforts was sporadic and ad hoc. Of the six current ATC system development efforts that we reviewed, four had security requirements, but only two of the four developed their security requirements based on a risk assessment. Without security requirements based on sound risk assessments, FAA cannot effectively protect future ATC systems from attack. Further, with no security requirements specified during systems design, any attempts to retrofit security features later will be increasingly costly and technically challenging.

As FAA modernizes and increases system interconnectivity, ATC systems will become more vulnerable, placing even more importance on FAA's ability to develop adequate security measures. These future vulnerabilities are well documented in FAA's information security mission need statement and also in reports completed by the President's Commission on Critical

[10]Volpe Transportation Systems Center NAS AIS Security Review, Final Report, October 1, 1996.

Infrastructure Protection. The mission need statement asserts that "information security is the FAA mission area with the greatest need for policy, procedural, and technical improvement. Immediate action is called for to develop and integrate information security into ATC systems." The President's Commission summary report concluded that the future ATC architecture appeared to have vulnerabilities and recommended that FAA act immediately to develop, establish, fund, and implement a comprehensive systems security program to protect the modernized ATC system from information-based and other disruptions, intrusions, and attacks. It further recommended that this program be guided by the detailed recommendations made in the National Airspace Systems vulnerability assessment.

Finally, FAA's management structure and implementation of policy for ATC computer security was not effective. Security responsibilities were distributed among three organizations, all of which have been remiss in their ATC security duties. The Office of Civil Aviation Security was responsible for developing and enforcing security policy, the Office of Air Traffic Services was responsible for implementing security policy for operational ATC systems, and the Office of Research and Acquisitions was responsible for implementing policy for ATC systems that are being developed. The Office of Civil Aviation Security had not adequately enforced FAA's policies that require the assessment of physical security controls at all ATC facilities and vulnerabilities, threats, and safeguards for all operational ATC computer systems. In addition, the Office of Air Traffic Services had not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards. Finally, the Office of Research and Acquisitions had not implemented the FAA policy that requires it to formulate requirements for security in specifications for all new ATC modernization systems.

FAA recently established a central security focal point, the National Airspace Systems Information Security (NIS) group, to develop additional security guidance (i.e., a security architecture, a security concept of operations, and security standards), to conduct risk assessments of selected ATC systems, to create a mechanism to respond to security incidents, and to provide security engineering support to ATC system development teams. This group has developed an action plan that describes each of its improvement activities, but it has not developed detailed plans or schedules to accomplish these tasks.

Establishing a central security focal point is a practice employed by leading security organizations. However, in order to be effective, the security focal point must have access to senior executives that are organizationally positioned to take action and effect change across organizational divisions. One approach for ensuring that a central group has such access at FAA would be to place it under a Chief Information Officer (CIO) who reports directly to the FAA Administrator. This approach is consistent with the Clinger-Cohen Act,[11] which requires that major federal departments and agencies establish CIOs who report to the department/agency head and are responsible for implementing effective information management.

FAA does not have a CIO reporting to the Administrator. Although the NIS group has access to certain key Associate Administrators (e.g., the Associate Administrator for Civil Aviation Security and the Associate Administrator for Research and Acquisitions), it does not have access to the management level that can effect change across organizational divisions, especially FAA's Administrator or Deputy Administrator. Thus, there is no assurance that the NIS group's guidance, once issued, will be adequately implemented and enforced, that results of its risk assessments will be acted upon, and that all security breaches will be reported and adequately responded to. Until existing ATC computer security policy is effectively implemented and enforced, operational and developmental ATC systems will continue to be vulnerable to compromise of sensitive information and interruption of critical services.

In our report, we recommended that FAA take a number of actions to improve its information security. For example, we recommended that FAA

- develop and execute a plan to inspect the 187 ATC facilities that have not been inspected in over 4 years and correct any weaknesses identified;
- correct identified physical security weaknesses at inspected facilities;
- ensure that specifications for all new ATC systems include security requirements based on detailed security assessments; and
- ensure the NIS group establishes detailed plans and schedules to develop a security architecture, a security concept of operations, and security standards and that these plans are implemented.

Finally, we recommended that FAA establish an effective management structure for developing, implementing, and enforcing ATC computer security policy. Given the importance and the magnitude of the

[11]The 1996 Clinger-Cohen Act, Public Law No. 104-106, section 5125, 110 Stat. 684 (1996).

information technology initiative at FAA, we expanded on our earlier recommendation that a CIO management structure similar to the department-level CIOs as prescribed in the Clinger-Cohen Act be established for FAA[12] by recommending that FAA's CIO be responsible for computer security. We further recommended that the NIS group report to the CIO and that the CIO direct the NIS group to implement its plans.

In contrast to State, the Department of Transportation's response to our recommendations was disappointing. The department only discussed its efforts for timely corrective actions pertaining to 1 of our 15 recommendations. It did not state what, if any, specific action it would take on the remaining 14 recommendations. This noncommitment is troubling considering that several of our recommendations are requesting that FAA adhere to its existing computer security policies.

Learning From Leading Organizations to Face the Challenges in Securing Systems

Poor computer security is a pervasive problem across government. Security problems are often dealt with on an ad hoc basis with too little attention given to systemic issues and problems that underlie individual security lapses or breaches. Frequently, responsibility for computer security is viewed as burdensome and relegated to (1) technical staff who do not have the resources or clout to prompt improvements and/or (2) line staff who lack the training and experience necessary to fully appreciate and mitigate computer security risks.

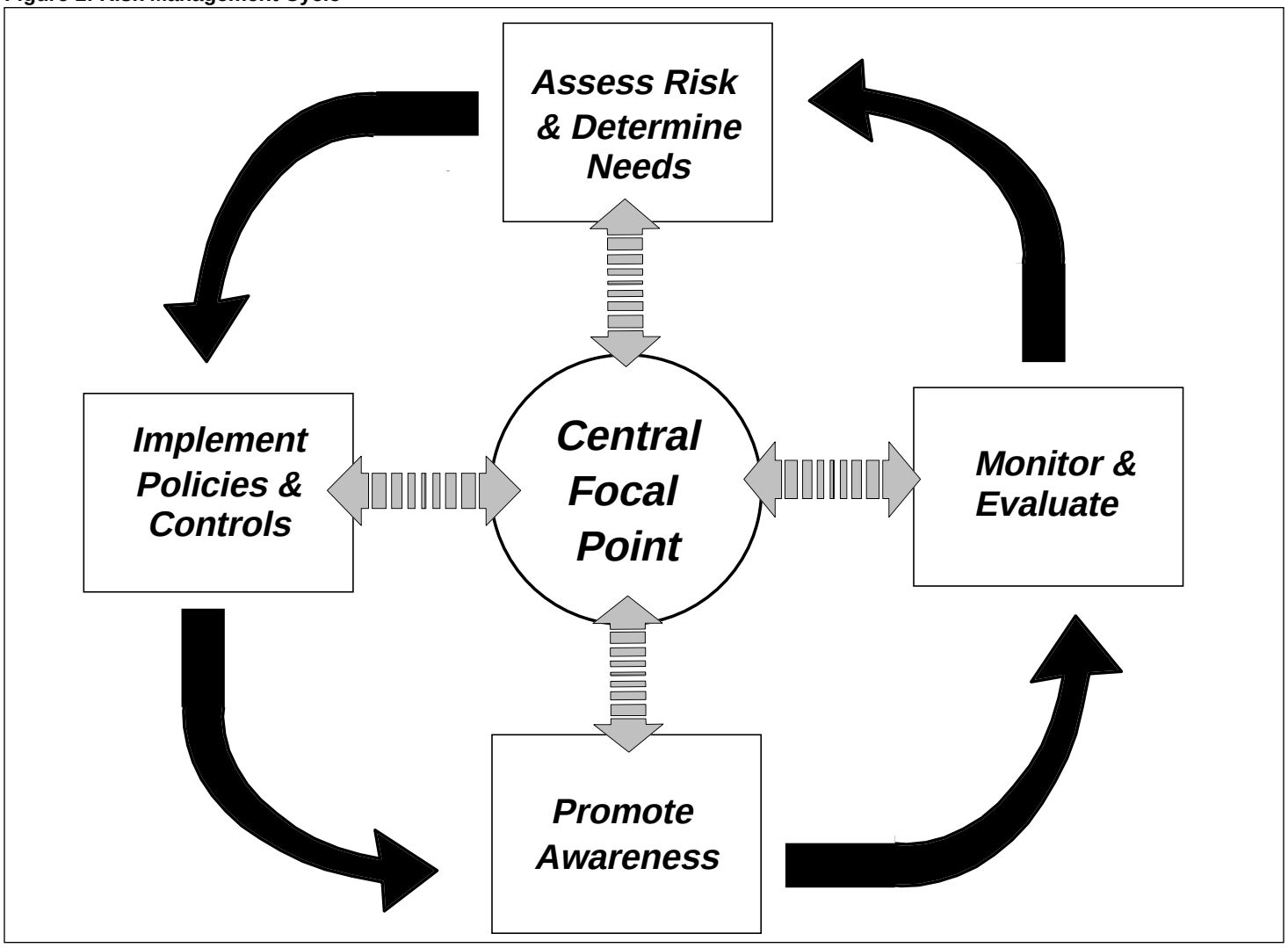
The problem is further complicated by the complex computing environment most agencies now must have to meet their operating needs. Many agencies have a conglomeration of mainframes, PCs, routers, servers, software applications, and external connections. Because absolute protection over these complex infrastructures is not feasible, developing effective information systems security involves an often intricate set of trade-offs between the (1) type and sensitivity of the information and operations to be protected, (2) vulnerabilities of the computers and networks, (3) various threats, including hackers, thieves, disgruntled employees, competitors, and, in the federal government's case, foreign adversaries and spies, (4) countermeasures available to combat the problem, and (5) costs. In making these trade-offs, agencies must understand the information security risks to their operations and assets, decide what they are going to do to defend themselves, and determine what risks they are willing to accept.

[12]Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, February 3, 1997) and Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, March 21, 1997).

We have found that many problems contribute to agencies' difficulties in successfully balancing the trade-offs necessary to establish effective computer security. However, an underlying factor is that senior agency officials have not established a framework for managing the information security risks associated with their operations. To better determine how leading organizations handled these trade-offs, we undertook a comprehensive study—at this Committee's request—of eight organizations with superior security programs. These organizations—regardless of business type, size, or management structure—had one overriding tenet: business "owners," not security experts, assumed both responsibility and accountability for computer security. At the same time, however, security specialists played a strong educational and advisory role and had the ability to elevate discussions to higher management levels when they believed that risks were not being adequately addressed.

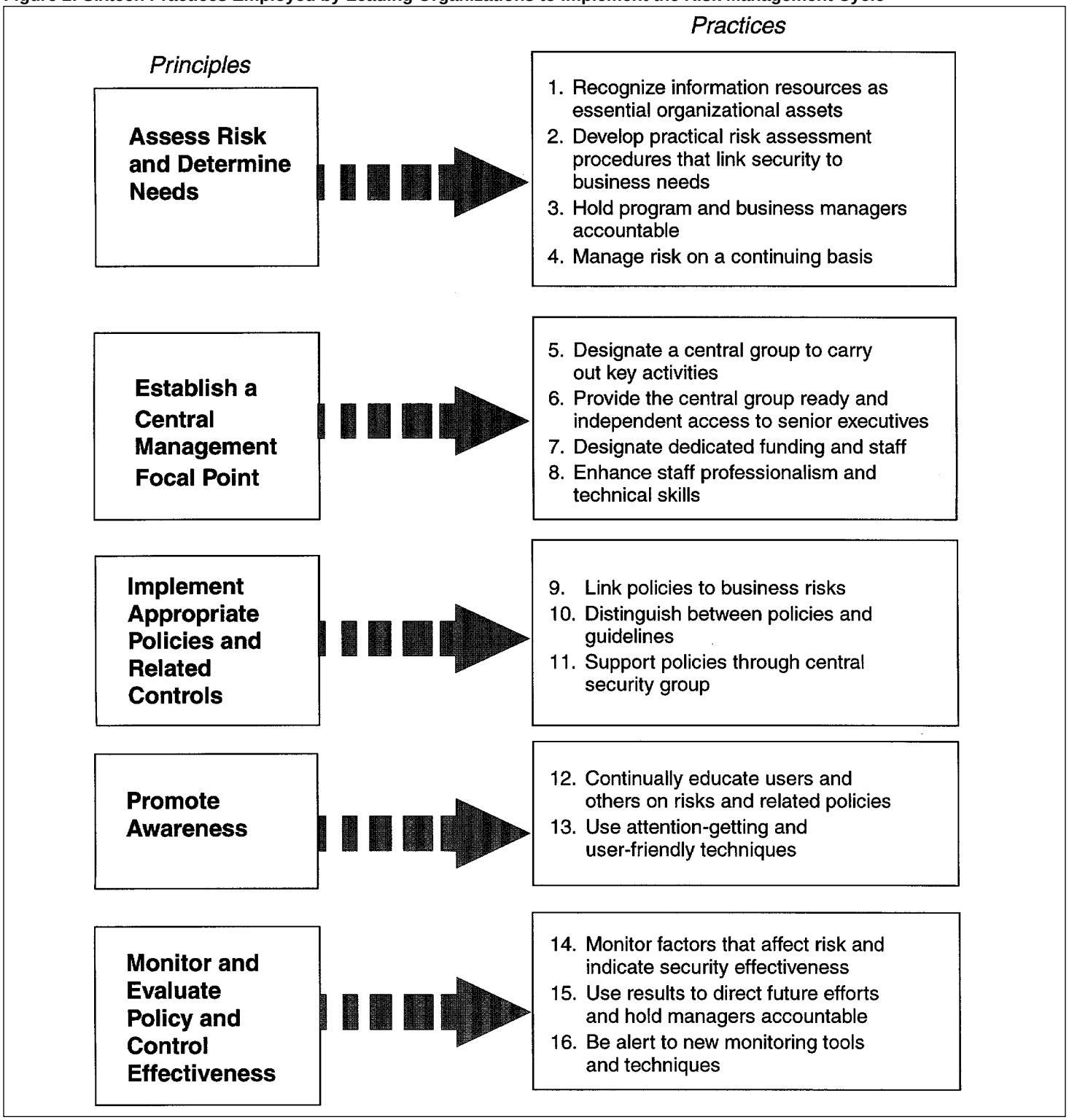
The organizations we studied managed their information security risks by implementing a continuing cycle of monitoring business risks, maintaining policies and controls, and monitoring operations. This cycle of activity parallels the process associated with managing the controls associated with any type of program. As illustrated in the figure below, all of these activities are coordinated through a central management office or group who served as consultants and facilitators to individual business units and senior management.

Figure 1: Risk Management Cycle



Each element of the risk management cycle, in turn, has a number of individual practices that these organizations followed to minimize risk.

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



We are pleased that the Committee is releasing the executive guide, which summarizes the results of our study, today.[13] We are equally pleased that the CIO Council has also endorsed our executive guide and the 16 practices followed by leading organizations. We are working with the Council and the Office of Management and Budget to encourage agencies to adopt these practices as additional guidance that can be used to enhance the government's ability to protect federal assets from fraud and misuse, inappropriate disclosure of sensitive information, and disruption of critical operations. And, of course, we are continuing our work for this Committee to review agency computer security programs and to identify solutions that target the underlying causes of security weaknesses. We are also working with the CIO Council to develop improved risk assessment practices and methodologies and have planned a significant amount of work in this area over the next 3 years.

This completes our testimony.

[13]Executive Guide: Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested