United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

September 1998

INFORMATION SECURITY

Serious Weaknesses Place Critical Federal Operations and Assets at Risk

GAO/AIMD-98-92

GAO

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

Accounting and Information
Management Division

B-278910

September 23, 1998

The Honorable Fred Thompson
Chairman
The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

In response to your request, this report describes (1) the overall state of federal information security based on recently issued audit reports and (2) executive branch efforts over the last 2 years to improve the federal government's performance in this important area. These efforts include actions by individual agencies, the Office of Management and Budget, and the Chief Information Officers Council, as well as initiatives outlined in the recently issued Presidential Decision Directive 63 on critical infrastructure protection. Many of these improvement efforts respond to recommendations made in our September 1996 report Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110), which was also developed at your request.

If you have any questions, please call me at (202) 512-2600. This report was developed under the direction of Robert F. Dacey, Director, Consolidated Audit and Computer Security Issues, and Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems. Major contributors to this report are listed in appendix IV.

Gene L. Dodaro
Assistant Comptroller General

Executive Summary

Purpose

Due to growing concerns about our government's reliance on inadequately protected information systems to support critical and sensitive operations, the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs asked GAO to (1) evaluate the effectiveness of federal information security practices based on the results of recent audits and (2) review efforts to centrally oversee and manage federal information security. This report describes the results of that analysis and outlines management practices that could improve the effectiveness of federal agency security programs.

Background

Federal agencies rely on computers and electronic data to perform functions that are essential to the national welfare and directly affect the lives of millions of individuals. More and more, these functions, which include national defense, tax collection, benefits payments, and law enforcement, depend on automated, often interconnected, systems and on electronic data rather than on manual processing and paper records. This shift has resulted in a number of benefits so that information can now be processed quickly and communicated almost instantaneously among federal offices, departments, and outside organizations and individuals. In addition, vast amounts of useful data are at the disposal of anyone with access to a personal computer, a modem, and telephone.

However, the government's increasing reliance on interconnected systems and electronic data also increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services. The same factors that benefit federal operations—speed and accessibility—also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on these operations from remote locations for purposes of fraud or sabotage, or other malicious or mischievous purposes.

Threats of such actions are increasing, in part, because the number of individuals with computer skills is increasing and because intrusion, or "hacking," techniques have become readily accessible through media such as magazines and computer bulletin boards. In addition, natural disasters and inadvertent errors by authorized computer users can have negative consequences if information resources are poorly protected.

Gauging the level of risk is difficult because summary data on computer security incidents and related damage are incomplete. However, break-ins and damage of varying levels of significance have been acknowledged in

both the public and private sectors, and media reports on intrusions, fraud, and sabotage abound. In a recent survey conducted by the Computer Security Institute in cooperation with the Federal Bureau of Investigation, 64 percent of the 520 respondents, which were from both the private and public sectors, reported computer security breaches within the last 12 months—a 16 percent increase in security breaches over those reported in a similar survey in 1997. While many of the survey respondents did not quantify their losses, those that did cited losses totaling $136 million.[1] In an October 1997 report entitled Critical Foundations: Protecting America's Infrastructures, the President's Commission on Critical Infrastructure Protection described the potentially damaging implications of poor information security from a national perspective, noting that computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways that cannot yet be fully conceived.

To guard against such problems, federal agencies must take steps to understand their information security risks and implement policies and controls to reduce these risks, but previous reports indicate that agencies have not adequately met this responsibility. In September 1996, GAO reported that a broad array of federal operations were at risk due to information security weaknesses and that a common underlying cause was inadequate security program management. In that report, GAO recommended that the Office of Management and Budget (OMB) play a more proactive role in leading federal improvement efforts, in part through its role as chair of the Chief Information Officers (CIO) Council. Subsequently, in a February 1997 series of reports to the Congress, GAO designated information security as a new governmentwide high-risk area.[2] More recently, in its March 31, 1998, report on the federal government's consolidated financial statements, GAO reported that widespread computer control deficiencies also contribute to problems in federal financial management because they diminish confidence in the reliability of financial management data.[3]

Results in Brief

The expanded amount of audit evidence that has become available since mid-1996 describes widespread and serious weaknesses in the federal government's ability to adequately protect (1) federal assets from fraud

[1]"Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey," March 4, 1998.

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

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

and misuse, (2) sensitive information from inappropriate disclosure, and (3) critical operations, including some affecting public safety, from disruption. Significant information security weaknesses were reported in each of the 24 largest federal agencies, with inadequately restricted access to sensitive data being the most widely reported problem. This and the other types of weaknesses identified place critical government operations, such as national defense, tax collection, law enforcement, and benefit payments, as well as the assets associated with these operations, at great risk of fraud, disruption, and inappropriate disclosures. In addition, many intrusions or other potentially malicious acts could be occurring but going undetected because agencies have not implemented effective controls to identify suspicious activity on their networks and computer systems.

Individual agencies have not yet done enough to effectively address these problems. Specifically, agency officials have not instituted procedures for ensuring that risks are fully understood and that controls implemented to mitigate risks are effective. Implementing such procedures as part of a proactive, organization-wide security management program is essential in today's interconnected computing environments.

Similarly, agency performance in this area is not yet being adequately managed from a governmentwide perspective, although some important steps have been taken. The CIO Council, under OMB's leadership, designated information security as a priority area in late 1997 and, since then, has taken some steps to develop a preliminary strategy, promote awareness, and identify ways to improve a federal incident response program developed by the National Institute of Standards and Technology (NIST). In May 1998, Presidential Decision Directive (PDD) 63 on critical infrastructure protection was issued. PDD 63 acknowledged computer security as a national security risk and established several 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. At the close of GAO's review in August 1998, it was too early to determine how the Directive's provisions would be implemented and how they would relate to other ongoing efforts, such as those initiated by the CIO Council.

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.

Principal Findings

Significant Weaknesses at 24 Major Agencies Place Critical Operations at Risk

Audit reports issued from March 1996 through August 1998 identified significant information security weaknesses in each of the 24 agencies covered by the analysis. The most widely reported type of weakness was poor control over access to sensitive data and systems. This type of weakness makes it possible for an individual or group to inappropriately modify or destroy sensitive data or computer programs or inappropriately obtain or disclose confidential information for malicious 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 minimal computer and telecommunications resources and expertise.

These weaknesses place a broad range of critical operations and assets at great risk of fraud, misuse, and disruption. For example, weaknesses at the Department of Defense increase the vulnerability of various military operations that support the Department's warfighting capability, and weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections.

In addition, information security weaknesses place an enormous amount of highly sensitive data at risk of inappropriate disclosure. For example, weaknesses at agencies such as the Internal Revenue Service, the Health Care Financing Administration, the Social Security Administration, and the Department of Veterans Affairs place sensitive tax, medical, and other personal records at risk of disclosure.

As significant as these reported weaknesses are, it is likely that the full extent of control problems at individual agencies has not yet surfaced

because key areas of controls at many agencies have not been assessed. In particular, agency managers, who are primarily responsible for ensuring adequate security, have not fully evaluated the adequacy of their computer-based controls. In addition, audits at most agencies have not yet fully covered controls associated with operating system software, which are critical to the security of all of the applications the systems support. In agencies where this control area was reviewed, weaknesses were always identified.

Improved Security Program Planning and Management Needed at Individual Agencies

Poor security program planning and management continue to be fundamental problems. Agencies have not yet developed effective procedures for assessing computer security risks, determining which risks are significant, assigning responsibility for taking steps to reduce risks, and ensuring that these steps remain effective. Security planning and management deficiencies were reported for 17 of the 24 agencies included in GAO's analysis and numerous recommendations have been made to address specific agency deficiencies.

To identify potential solutions to this problem, GAO studied the security management practices of eight organizations known for their superior security programs. These organizations included two financial institutions, a retailer, an equipment manufacturing company, a state university, a state agency, a regional electric utility, and a computer vendor. GAO found that these organizations managed their information security risks through a cycle of risk management activities, and it identified 16 specific practices that supported these risk management principles.

These practices involve (1) establishing a central security management focal point, (2) assessing risk, (3) selecting and implementing cost-effective policies and controls, (4) promoting awareness, and (5) continually evaluating and improving control effectiveness. They also emphasize the importance of viewing information security program management as an integral component of managing agency operations and of involving both program managers and technical experts in the process.

GAO published the findings from this study in the May 1998 executive guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), which has been endorsed by the Federal CIO Council. The guide's findings are summarized in chapter 3 of this report.

The security management practices described in GAO's executive guide are most likely to be successful if they are implemented as part of broader improvements to information technology management. Such improvements are underway across government due to specific information technology management reforms mandated by the Paperwork Reduction Act amendments of 1995 and the Clinger-Cohen Act of 1996.

Initiatives to Improve Central Coordination and Management Need to Provide a Comprehensive Strategy

Individual agencies are primarily responsible for the security of their information resources, but central management also is important to (1) ensure that federal executives understand risks to their operations, (2) monitor agency performance in mitigating these risks, (3) facilitate implementation of any needed improvements, and (4) address issues that affect multiple agencies. Under the Paperwork Reduction Act, this oversight responsibility lies with OMB.

Since September 1996 when GAO reported that OMB needed to strengthen its oversight of agency practices, the CIO Council, under OMB's leadership, has become a component of the administration's efforts to address federal information security problems and has taken some actions in this regard. Specifically, during 1997, the Council designated information security as one of six priority areas and, late in the year, established a Security Committee. Since then, the Committee has (1) developed a preliminary plan for addressing various aspects of the problem, (2) established links with other federal entities involved in security issues, (3) held a security awareness day for federal CIOs, deputy CIOs, and security officers, and (4) developed plans for reorienting the Federal Computer Incident Response Capability (FedCIRC), a program initiated by NIST to assist agencies in improving their security incident response capabilities and other aspects of their security programs.

In addition, OMB has continued to monitor selected agency system-related projects, many of which have significant security implications. However, neither OMB nor the CIO Council has yet developed a program for comprehensively overseeing and managing the security of critical federal operations by ensuring that agency programs are adequately evaluated and that the results are used to measure and prompt improvements, as recommended in GAO's September 1996 report.

Concurrent with OMB and CIO Council efforts during late 1997 and early 1998, the administration developed and issued PDD 63 in response to recommendations made by the President's Commission on Critical

Infrastructure Protection. The Directive acknowledges computer security risk as a national security risk, addresses a range of national infrastructure protection issues, and includes several provisions intended to ensure that critical federal computer, or "cyber-based," systems are protected from attacks by our nation's enemies. Also, it establishes a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who reports to the President through the Assistant to the President for National Security Affairs; a Critical Infrastructure Coordination Group; and a Critical Infrastructure Assurance Office within the Department of Commerce. The Directive outlines planned actions pertaining to federal information security, which include:

- requiring each federal department and agency to develop a plan for protecting its own critical infrastructure, including its cyber-based systems;
- reviewing existing federal, state, and local entities charged with information assurance tasks;
- enhancing collection and analysis of information on the foreign information warfare threat to our critical infrastructures;
- establishing 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;
- assessing U.S. Government systems' vulnerability to interception and exploitation; and
- incorporating agency infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

Though some of these efforts have begun, at this early stage of implementation, it is unclear how the provisions outlined in the Directive will be implemented and how they will be coordinated with other related efforts, such as those of the CIO Council.

Conclusion

Since September 1996, the need for improved federal information security has received increased visibility and attention. Important efforts have been initiated to address this issue, but more effective actions are needed both at the individual agency level and at the governmentwide level. Many aspects of the recommendations GAO made in September 1996 are still applicable. In particular, a comprehensive governmentwide strategy needs to be produced. The CIO Council's efforts during late 1997 and the first half of 1998, as well as issuance of PDD 63 in May 1998, indicate that senior

federal officials are increasingly concerned about information security risks, both to federal operations as well as to privately controlled national infrastructures, and are now moving to address these concerns. Coordinated efforts throughout the federal community, as envisioned by PDD 63, will be needed to successfully accomplish the objectives of these efforts and substantively improve federal information security. It is especially important that a governmentwide strategy be developed that clearly defines and coordinates the roles of new and existing federal entities in order to avoid inappropriate duplication of effort and ensure governmentwide cooperation and support.

Recommendation

GAO recommends that the Director of OMB and the Assistant to the President for National Security Affairs ensure that the various existing and newly initiated efforts to improve federal information security are coordinated under a comprehensive strategy. 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.

Agency Comments and Our Evaluation

In commenting on a draft of this report, OMB's Acting Deputy Director for Management stated that OMB and the CIO Council, working with the National Security Council, have developed a plan to address the PDD 63 provision that the federal government serve as a model for critical infrastructure protection and to coordinate the new requirements of the

PDD with the existing requirements of the various laws pertaining to federal information security. The comments further 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. Also described are plans for a CIO Council-sponsored interagency security assist team that will review agency security programs. Regarding our conclusion that many aspects of the recommendations in our September 1996 report are still applicable, OMB reiterated its concern that the 1996 report's "overemphasis on OMB's role could distract program managers in the Federal agencies from their primary responsibility for assuring information security." The full text of OMB's comments is reprinted in appendix III.

OMB's comments indicate that it, the CIO Council, and the National Security Council are moving to coordinate their responsibilities and beginning to develop the comprehensive strategy that is needed. Based on the description provided, the plans being developed include several key elements, most notably a means of evaluating agency performance. These plans were still being finalized at the close of our work and were not yet available for our review. Accordingly, we are not able to comment on their content, scope, and detail, or whether they will be effective in improving federal information security.

Regarding OMB's concern that we have overemphasized its role, we agree that agency managers are primarily responsible for the security of their operations. Increased attention and support from central oversight, if done effectively, should not distract agencies from their responsibilities in this area. On the contrary, active oversight of agency performance is more likely to have the effect of emphasizing the agency managers' accountability and providing more visibility for agencies that are achieving their information assurance goals as well as those that are falling short.

Contents

Table

Figure

Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
DOD	Department of Defense
FAA	Federal Aviation Administration
FedCIRC	Federal Computer Incident Response Capability
FMFIA	Federal Managers' Financial Integrity Act
IG	Inspector General
GAO	General Accounting Office
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
SSA	Social Security Administration
VA	Department of Veterans Affairs

Introduction

This report provides a summary analysis of recently reported information security weaknesses at federal agencies and describes management practices that federal agencies can adopt to help improve their security programs. It also describes centralized efforts to oversee and manage federal information security from a governmentwide perspective.

The vulnerabilities associated with our nation's reliance on interconnected computer systems are a growing concern. At the federal level, such systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. Because of the importance of establishing and maintaining adequate security over federal operations, Senators Fred Thompson and John Glenn, Chairman and Ranking Minority Member, respectively, of the Senate Committee on Governmental Affairs, have undertaken an effort to address the various management, technical, and operational aspects of this problem. As part of that effort, they requested that we (1) summarize the effectiveness of federal information security, based on recently issued audit reports, (2) describe actions agencies can take to improve their security programs, and (3) evaluate actions taken by the Office of Management and Budget (OMB) and the federal Chief Information Officers (CIO) Council to address federal information security problems. This resulting report is one of several reviews that Chairman Thompson and Senator Glenn have requested as part of their ongoing oversight of federal information security and other aspects of information technology management. Related GAO reports are listed in appendix I.

Computers and Electronic Data Are Indispensable to Federal Operations

Federal agencies perform important functions that are essential to the national welfare and directly affect the lives of millions of individuals everyday. More and more, these functions, which include national defense, tax collection, import control, benefits payments, and law enforcement, depend on automated, often interconnected, systems and on electronic data rather than on manual processing and paper records. The benefits of this shift are increasingly obvious—information can be processed quickly and communicated almost instantaneously among federal offices, departments, and outside organizations and individuals. In addition, vast amounts of data are at the disposal of anyone with access to a personal computer, a modem, and telephone.

However, the government's increasing reliance on interconnected systems and electronic data also increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and

services. The same factors that benefit federal operations—speed and accessibility—also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on these operations from remote locations for purposes of fraud or sabotage, or other malicious or mischievous purposes. Threats of such actions are increasing, in part, because the number of individuals with computer skills is increasing and because intrusion, or "hacking," techniques have become readily accessible through magazines and on computer bulletin boards. In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected.

Gauging the risk is difficult because summary data on computer security incidents and related damage are incomplete. However, in an October 1997 report entitled Critical Foundations: Protecting America's Infrastructures, the President's Commission on Critical Infrastructure Protection described the potentially devastating implications of poor information security from a national perspective, noting that computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive. According to a recent statement by the Director of the National Security Agency, attacks on public and private systems occur everyday. For example, in February 1998, hackers used tools and techniques readily available on Internet bulletin boards to attack systems at the Department of Defense. Media reports on intrusions, fraud, and sabotage abound, and, in a recent survey conducted by the Computer Security Institute in cooperation with the Federal Bureau of Investigation, 64 percent of the 520 respondents from the private and public sector reported computer security breaches within the last 12 months. This is a 16-percent increase in security breaches over those reported in a similar survey in 1997 and a 22-percent increase over those reported in 1996.[1]

To guard against such problems, federal agencies, like other computer-dependent organizations, must take steps to understand their information security risks and implement policies and controls to reduce these risks. Specifically, federal agencies must protect the integrity and, in some cases, the confidentiality of the enormous amounts of sensitive data they maintain, such as personal information on individuals, financial transactions, defense inventories, operational plans, and regulatory inspection records. In addition, they must take steps to ensure that

[1]"Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey," March 4, 1998.

computerized operations supporting critical government functions are not severely disrupted.

Previous Reports Have Identified Significant Security Problems

Although the government's reliance on computers and telecommunications has been rapidly growing, reports over the last few years indicate that federal operations and data are inadequately protected and that these problems are serious and pervasive. In September 1996, we reported that, since September 1994, serious weaknesses had been reported for 10 of the largest 15 federal agencies.[2] In that report we concluded that poor information security was a widespread federal problem with potentially devastating consequences, and we recommended that OMB play a more proactive role in overseeing agency practices and managing improvements, in part through its role as chair of the CIO Council. Subsequently, in February 1997, in a series of reports to the Congress, we designated information security as a new governmentwide high-risk area.[3] Most recently, in our March 31, 1998, report on the federal government's consolidated financial statements, we reported that widespread and serious computer control weaknesses affect virtually all federal agencies and significantly contribute to many material deficiencies in federal financial management.[4] In that report, we also noted that these weaknesses place enormous amounts of federal assets at risk of fraud and misuse, financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

During 1996 and 1997, federal information security was also 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, expediting efforts to facilitate the use of encryption, developing risk assessment

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

methods, measuring performance, and elevating threat assessments as a foreign intelligence priority.

A number of factors contribute to poor federal information security including insufficient awareness and understanding of risks, a shortage of staff with needed technical expertise, a lack of systems and security architectures to facilitate implementation and management of security controls, and various problems associated with the availability and use of specific technical controls and monitoring tools. All of these are important; however, an underlying theme that was identified in our September 1996 report is a lack of security program management and oversight to ensure that risks are identified and addressed and that controls are working as intended.

Responsibilities Outlined in Laws and Guidance

The need to protect sensitive federal data maintained on automated systems has been recognized for years in various laws and in federal guidance. The Privacy Act of 1974, as amended; the Paperwork Reduction Act of 1980, as amended; and the Computer Security Act of 1987 all contain provisions requiring agencies to protect the confidentiality and integrity of the sensitive information that they maintain. The Computer Security Act (Public Law 100-235) defines sensitive information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

In accordance with the Paperwork Reduction Act of 1980 (Public Law 96-511), OMB is responsible for developing information security policies and overseeing agency practices. In this regard, OMB has provided guidance for agencies in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Since 1985, this circular has directed agencies to implement an adequate level of security for all automated information systems that ensures (1) effective and accurate operations and (2) continuity of operations for systems that support critical agency functions. The circular establishes a minimum set of controls to be included in federal agency information system security programs and requires agencies to periodically review system security. Responsibility for developing technical standards and providing related guidance for

sensitive data belongs primarily to the National Institute of Standards and Technology (NIST), under the Computer Security Act.

The Clinger-Cohen Act of 1996 recently reemphasized OMB, NIST, and agency responsibilities regarding information security under a broader set of requirements aimed at improving information technology management in general. In particular, the act stipulated that agency heads are directly responsible for information technology management, including ensuring that the information security policies, procedures, and practices of their agencies are adequate. The act also required the appointment of a CIO for each of the 24 largest federal agencies to provide the expertise needed to implement needed reforms. Subsequently, in July 1996, the President established the CIO Council, chaired by OMB, to address governmentwide technology issues and advise OMB on policies and standards needed to implement legislative reforms. Council members include CIOs and Deputy CIOs from each of the major agencies.

The adequacy of controls over computerized data and the management of these controls are also addressed indirectly by the following additional laws:

- The Federal Managers' Financial Integrity Act (FMFIA) of 1982 requires agency managers to annually evaluate their internal control systems and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations.
- The Chief Financial Officers (CFO) Act of 1990, as expanded by the Government Management Reform Act of 1994, requires agency CFOs to develop and maintain financial management systems that provide complete, reliable, consistent, and timely information. Under the act, major federal agencies prepare annual financial statements and have them audited by their respective inspectors general. In practice, such audits generally include evaluating and testing controls over the security of automated financial management systems.
- The Federal Financial Management Improvement Act of 1996 requires auditors to report whether agency financial management systems comply with certain established financial management systems requirements. OMB guidance to agency CFOs and IGs lists these systems requirements, which include security over financial systems provided in accordance with OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Agency managers are responsible for developing remediation plans to address the problems noted by the auditors.

- The Government Performance and Results Act of 1993 requires agencies to establish goals for program performance, measure results, and report annually on program performance to the President and the Congress.

In May 1998, Presidential Decision Directives 62 and 63 established additional requirements for ensuring protection of our nation's critical infrastructures from both physical and "cyber," or computer-based, threats. At the close of our fieldwork in August 1998, it was too early to determine how these directives would be implemented. However, the provisions pertaining to federal agency information security that are specified in Directive 63 are summarized in chapter 4. Presidential Decision Directive 62, which pertains to counter-terrorism responsibilities, is classified and, therefore, is not discussed in this report.

Objectives, Scope, and Methodology

The objectives of this report are to

- describe the extent of federal information security problems and the associated risks based on reports issued since March 1996,
- identify management actions that could effect significant and long-term improvements in information security at the individual agency level, and
- evaluate governmentwide efforts to improve information security, especially actions taken since September 1996 by OMB and the CIO Council, and identify needed additional actions.

To describe the extent of information security problems and associated risks, we analyzed findings from over 80 GAO and agency reports, including inspector general (IG) reports, issued from March 1996 through September 1998. These included some reports for which distribution has been restricted because they discuss sensitive aspects of agency operations. Although we considered the results of these restricted reports when developing summary data on agency weaknesses, the related findings are not discussed in detail nor the agency identified. The reports we considered pertained to the 24 federal departments and agencies covered by the CFO Act. Together these departments and agencies accounted for about 99 percent of the total reported federal net outlays in fiscal year 1997. The reports we analyzed, excluding those that are restricted, are listed in appendixes I and II.

In analyzing reported findings, we categorized them into six basic areas of general control: security program planning and management, access control, application program change control, segregation of duties,

operating systems security, and service continuity. These six areas of general controls provide a framework for comprehensively evaluating information security. The six categories are defined and described in chapter 2.

To identify management actions that could effect fundamental improvements in security at individual agencies, we summarized the results of our recent study of information security program management practices at leading organizations. We performed this study because previous audits had shown that poor security program management was an underlying cause of information security control weaknesses. In May 1998, we published the results of this study as an executive guide entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68).

To assess OMB's leadership and coordination of federal information security efforts, we met with officials from OMB's Office of Information and Regulatory Affairs to discuss their activities related to information security and progress on recommendations made in our report Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996). We also discussed the information security-related activities of the federal CIO Council with members of the Council's Security Committee and reviewed related documentation, such as meeting minutes and the CIO Council's January 1998 governmentwide strategic plan for information resources management.

We also obtained and reviewed Presidential Decision Directive 63, which was issued May 22, 1998, late in our review. This directive specifies requirements for protecting our nation's critical infrastructures and includes provisions pertaining to federal agency information security.

Our review was conducted from December 1997 through August 1998 in accordance with generally accepted government auditing standards. One of the reports we relied on, VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175), is being issued in September 1998. However, a complete draft was available at the close of our review in August. OMB provided written comments on a draft of this report, which are discussed in the "Agency Comments and Our Evaluation" section in chapter 4 and reprinted in appendix III.

Related GAO Efforts

In addition to this report, we have worked with the Congress, primarily the Senate Committee on Governmental Affairs, to pursue a comprehensive strategy for addressing the federal information security problems. This strategy involves supplementing our audit work with research projects and other actions to promote and provide support for federal efforts in this area. This strategy comprises the following activities:

- To assess the effectiveness of federal information security and assist the Congress in its oversight role, we are continuing to perform audits at selected individual agencies and develop specific recommendations for improvement. Some of these evaluations are performed as part of our financial statement audits at individual agencies and some pertain to nonfinancial mission-critical systems.
- To assist agency inspectors general in conducting or arranging for information security audits, we began an extensive effort during 1997 to evaluate such audit efforts at each of 24 major federal agencies. We performed, and will continue to perform, this work in conjunction with our annual audits of the consolidated financial statements of the federal government, which are required under the CFO Act as expanded by the Government Management Reform Act. At many of these agencies, we have provided extensive on-site guidance to the inspector general staff to ensure that we could rely on their audit conclusions.
- To promote more comprehensive audits of federal information security, in August 1997, we issued an exposure draft of our Federal Information System Controls Audit Manual (GAO/AIMD-12.19.6), which describes a methodology for evaluating federal agency information security programs. This methodology has guided our own audit work for several years and has recently been adopted by many agency inspectors general.
- To assist in improving the expertise of federal audit staff, we have engaged contractors and partnered with organizations, such as the Information Systems Audit and Control Association, to offer technical training sessions for GAO and IG staff involved in evaluating computer-based controls.
- To promote a broader understanding among federal managers of the practices that make an information security program successful, during 1997, we studied the practices of eight nonfederal organizations and developed an executive guide that summarizes the results. This guide, entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68) was published in May 1998. We are now working with agencies, including OMB, and the CIO Council to encourage agencies to implement these practices.
- To promote more effective central leadership, oversight, and coordination, we are continuing to monitor and work with OMB, the CIO Council, NIST, and

others with a governmentwide role regarding information security, including entities established under Presidential Decision Directive 63 to protect our nation's critical infrastructures.

- To assist the Congress, we are continuing to provide status reports on information security as a high-risk issue and information on related topics, as requested.

Significant Weaknesses Identified at All Major Agencies

Evaluations of computer security published since March 1996 present a disturbing picture of the federal government's lack of success in protecting its assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption. Significant information security weakness were identified in each of the 24 agencies covered by our analysis—agencies that in fiscal year 1997 accounted for 99 percent of reported federal net outlays. These weaknesses place a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they place an enormous amount of highly sensitive data, much of it on individual taxpayers and beneficiaries, at risk of inappropriate disclosure.

Weaknesses were reported in a variety of areas that we have categorized into six areas of "general controls." General controls are 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. The most widely reported weakness was poor control over access to sensitive data and systems. This type of weakness makes 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 minimal computer and telecommunications resources and expertise.

The full extent of control problems is not known because all six of the general control areas were reviewed at only 9 of the 24 agencies. In particular, most audits have not yet covered controls associated with system software, which are critical to the security of all applications supported by a system. In agencies where this control area was reviewed, weaknesses were always found, as shown in table 1.

Table 1 provides an overview of the types of weaknesses reported throughout the government, as well as the gaps in audit coverage. The pages following Table 1 describe (1) the risks these weaknesses pose to major federal operations and (2) common types of deficiencies identified in each of the six general control categories.

Table 2.1: Areas of Information Security Weakness Reported for the 24 Largest Agencies

	Number of agencies		
General control area	Significant weakness identified	No significant weakness identified	Area not reviewed
Entitywide security program planning and management	17	0	7
Access controls	23	0	1
Application software development and change controls	14	4	6
Segregation of duties	16	1	7
System software controls	9	0	15
Service continuity controls	20	0	4

Note: Most of the audits used to develop this table were performed as part of financial statement audits. At some agencies with primarily financial-related missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at other agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits used to develop this table 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 evaluating systems supporting nonfinancial operations. Nevertheless, at agencies where computer-based controls over nonfinancial operations have been audited, similar weaknesses have been identified.

Examples of Weaknesses at Individual Agencies Highlight Risks

To understand the significance of the weaknesses summarized in table 1, 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. Descriptions of reported weaknesses and related risks to selected major federal operations follow.

Department of the Treasury

The Department of the Treasury, which includes the Internal Revenue Service; U.S. Customs Service; Bureau of the Public Debt; Financial Management Service; and Bureau of Alcohol, Tobacco, and Firearms; relies on computer systems to process, collect or disburse, and account for over a trillion dollars in federal receipts and payments annually. In addition, the department's computers handle enormous amounts of highly sensitive data associated with taxpayer records and law enforcement operations and support operations critical to financing the federal government, maintaining the flow of benefits to individuals and organizations, and controlling imports and exports.

Protecting these operations and assets is essential to the welfare of our nation. However, weaknesses have been reported for several of Treasury's major bureaus, and, in some cases, these weaknesses have been outstanding for years. For example:

- In March 1998, the Treasury IG reported that deficiencies in the effectiveness of computer-based controls in multiple bureaus constituted a material weakness in the department's internal control structure and increased the risk that unauthorized individuals could intentionally or inadvertently add, alter, or delete sensitive data and programs.[1]
- In three 1997 reports,[2] we identified a wide range of continuing serious weaknesses in IRS systems, including inadequate controls over employee browsing of taxpayer records, an area that has received considerable attention for several years and was recently addressed by legislation specifying penalties for such browsing.[3]
- In March 1998, the Treasury IG reported Customs Service weaknesses associated with systems supporting trade, financial management, and law enforcement functions. Many of these weaknesses had been reported annually since 1994.[4]

Numerous recommendations have been made to Treasury bureaus over the years to correct these weaknesses, and many corrective actions are underway. In particular, IRS recently began a broad effort to strengthen its overall security program by centralizing responsibility for security issues within a newly created executive-level office and increasing investments in physical security. Further, the Financial Management Service concurred with our recommendations and is developing corrective action plans.

Department of Defense

The Department of Defense (DOD) relies on a vast and complex information infrastructure to support critical operations such as designing weapons, identifying and tracking enemy targets, paying soldiers, mobilizing reservists, and managing supplies. Indeed, its very warfighting

[1]Report on the Department of the Treasury's Fiscal Year 1997 Custodial Schedules and Administrative Statements (OIG-98-066, March 30, 1998), as included in the Department of the Treasury's Accountability Report for Fiscal Year 1997.

[2]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); Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997).

[3]Taxpayer Browsing Protection Act (Public Law 105-35).

[4]Department of the Treasury's Inspector General Report: Report on the U.S. Customs Service's Fiscal Years 1997 and 1996 Financial Statements (OIG-98-050, March 5, 1998).

capability is dependent on computer-based telecommunications networks and information systems. Defense's computer systems are particularly susceptible to attack through connections on the Internet, which Defense uses to enhance communication and information sharing.

In May 1996, we reported that attacks on Defense computer systems were a serious and growing threat.[5] The exact number of attacks could not be readily determined because tests showed that only a small portion were actually detected and reported. However, the Defense Information Systems Agency estimated that attacks numbered in the hundreds of thousands per year, were successful 65 percent of the time, and that the number of attacks was doubling each year. At a minimum, these attacks are a multimillion dollar nuisance to Defense. At worst, they are a serious threat to national security. According to Defense officials, attackers have obtained and corrupted sensitive information—they have stolen, modified, and destroyed both data and software. They have installed unwanted files and "back doors" which circumvent normal system protection and allow attackers unauthorized access in the future. They have shut down and crashed entire systems and networks, denying service to users who depend on automated systems to help meet critical missions. Numerous Defense functions have been adversely affected, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll. In March 1998, DOD announced that it had recently identified a series of organized intrusions, indicating that such events continue to be a problem.

The same weaknesses that allow attacks from outsiders could also be exploited by authorized users to commit fraud or other improper or malicious acts. In fact, a knowledgeable insider with malicious intentions can be a more serious threat to many operations since he or she is more likely to know of system weaknesses and how to disguise inappropriate actions.

Subsequent reports have identified a broad array of specific control weaknesses that increase the risks of damage from such attacks, as well as from malicious acts and inadvertent mistakes by authorized users. For example, in September 1997, we reported that Defense had not adequately (1) controlled the ability of computer programmers to make changes to systems supporting the Military Retirement Trust Fund, (2) controlled access to sensitive information on pension fund participants, or

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

(3) developed or tested a comprehensive disaster recovery plan for the sites that process Fund data. These weaknesses expose sensitive data maintained by these systems to unnecessary risk of disclosure and, should a disaster occur, there is no assurance that the operations supported by these facilities could be restored in a timely manner.[6] Similarly, In October 1997, the Defense IG reported serious authentication and access control weaknesses associated with a system that, in fiscal year 1996, maintained contract administration and payment data associated with a reported 387,000 contracts for which the reported value was over $810 billion.[7] Weaknesses in other areas, too sensitive to be reported publicly, pose risks of more serious consequences.

Reports to DOD have included numerous recommendations related to specific control weaknesses as well as the need for improved security program management. DOD is taking a variety of steps to address these problems and is establishing the Departmentwide Information Assurance Program to improve and better coordinate the information security-related activities of the military services and other DOD components.

Department of Health and Human Services

In August 1997 and April 1998, the Health and Human Services (HHS) IG reported serious control weaknesses affecting the reliability, confidentiality, and availability of data throughout the department.[8] Most significant were weaknesses associated with the Department's Health Care Financing Administration (HCFA), which, according to its reports, was responsible for processing health care claims for over 38 million beneficiaries and expending 84 percent of HHS' $340 billion fiscal year 1997 budget. HCFA relies on extensive data processing operations at its central office and about 60 contractors using multiple shared systems to collect, analyze and process personal health, financial, and medical data associated with about 853 million Medicare claims, annually.

In the 1997 report, the IG reported that Medicare contractors were not adequately protecting confidential personal and medical information associated with claims submitted. As a result, contractor employees could potentially browse data on individuals, search out information on

[6]Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997).

[7]General and Application Controls Over the Mechanization of Contract Administration Services System, DODIG, Report Number 98-007, October 9, 1997.

[8]Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1996 (A-17-96-0001, August 29, 1997) and Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1997 (A-17-98-0001, April 1, 1998).

acquaintances or others, and, possibly, sell or otherwise use this information for personal gain or malicious purposes. Similar conditions were reported in 1998.

In the 1998 report, the IG reported that data security remained a major concern at HCFA's central office. Auditor's tests showed that although HCFA corrected weaknesses found in the prior year, it was possible to gain access to the mainframe database and modify managed care production files. In addition, the IG found that users without specific authorization could potentially gain update access to those same files. Further, as reported in 1997 and 1998, because controls over operating system software were ineffective, knowledgeable individuals could surreptitiously modify or disable security controls without detection.

In both its 1997 and 1998 reports, the IG recommended that (1) systems access be properly controlled, passwords be granted consistent with assigned responsibilities, and passwords be periodically changed, (2) application development and program change control procedures be in place to protect against unauthorized changes, (3) computer-related duties be properly segregated, and (4) service continuity plans be kept current and periodically tested. HHS has recognized the need to protect the security of information technology systems and the data contained in them. Starting in 1997, HHS began to revise security policies and guidance and required each major operating division to develop and implement corrective action plans to address each major weakness identified in the August 1997 report.

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 $390 billion to 50 million beneficiaries. This represents about 25 percent of the $1.6 trillion in that year's federal expenditures. The administration also issues social security numbers and maintains earnings records and other personal information on virtually all U. S. citizens. According to SSA, no other public program or public-service entity directly touches the lives of 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. However, in November 1997, the Social Security Administration IG

reported widespread weaknesses in controls over access, continuity of service, and software program changes that unnecessarily place these assets and operations at risk.[9]

Access control weaknesses exposed the agency and its computer systems to external and internal intrusion, thus subjecting sensitive SSA information to potential unauthorized access, modification, or disclosure. Other weaknesses increased risks of introducing errors or irregularities into data processing operations and allowed some individuals to bypass critical controls, such as authorization and supervisory review.

Such weaknesses increase the risk that an 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.

In two separate letters issued to SSA management, the IG and its contractor made recommendations to address the weaknesses reported in November 1997. SSA agreed with the majority of the recommendations in the first letter and has developed related corrective action plans. The Administration is still reviewing the second set of recommendations and planning related corrective actions.

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 September 1998, we reported that general computer control weaknesses placed critical VA operations, such as financial management, healthcare delivery, benefit payments and life insurance services at risk of

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

misuse and disruption.[10] In addition, sensitive information contained in VA's systems, including financial transaction data and personal information on veteran medical records and benefit payments, was vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction—possibly occurring without detection.

VA operates the largest healthcare 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 noted significant problems related to the department's control and oversight of access to its systems. VA did not adequately limit the access of authorized users or effectively manage user identifications and passwords. The department also had not established effective controls to prevent individuals, both internal and external, from gaining unauthorized access to VA systems. VA's access control weaknesses were further compounded by ineffective procedures for overseeing and monitoring systems for unusual or suspicious access activities.

In addition, the department was not providing adequate physical security for its computer facilities, by not assigning duties in such a way as to segregate incompatible functions, controlling changes to powerful operating system software, or updating and testing disaster recovery plans to prepare its computer operations to maintain or regain critical functions in emergencies. Many of these access and other general computer control weaknesses were similar to weaknesses that had been previously identified by VA's Office of Inspector General and consultant evaluations.

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. An effective program would include guidance and procedures for assessing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls.

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

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, and (3) monitor and periodically report on the status of improvements to computer security throughout the department. In commenting on this report, VA agreed with these recommendations and stated that the department would immediately correct the identified computer control weaknesses and was developing plans to correct deficiencies previously identified by the VA IG and by internal evaluations.

Department of State

In May 1998, we reported that the Department of State did not have a program for comprehensively managing the information security risks associated with its many sensitive operations.[11] State relies on numerous decentralized information systems and networks to carry out its worldwide responsibilities and support business functions. Unclassified data stored in these systems are sensitive and make an attractive target for individuals and organizations desiring to learn about and damage State operations. For example, computerized information on Americans and Foreign Service Nationals, such as personnel records, pay data, private health records, and background investigation information about employees being considered for national security clearances could be useful to foreign governments wishing to build personnel profiles, and its disclosure might unnecessarily endanger State employees.

Despite its reliance on computers, State (1) lacked a central security management group to oversee and coordinate security activities, (2) did not routinely perform risk assessments so that its sensitive information could be protected based on its sensitivity, criticality, and value, (3) relied on a primary information security policy document that was outdated and incomplete, (4) did not adequately ensure that computer users were fully aware of risks and of their responsibilities for protecting sensitive information, and (5) lacked key controls for monitoring and evaluating the effectiveness of its security program, including procedures for responding to security incidents.

We also noted that State's information systems and the information contained within them were vulnerable to access, change, disclosure, disruption or even denial of service by unauthorized individuals. Our

[11]Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998).

penetration tests, which were designed to determine how susceptible State's systems were to unauthorized access, revealed that it was possible to access sensitive information. Further, these tests went largely undetected, further underscoring the department's serious vulnerability. As a result, individuals or organizations seeking to damage State operations, commit terrorism, or obtain financial gain could possibly exploit the department's information security weaknesses.

In our report to State, we made a variety of recommendations directed toward improving the department's management of its information security efforts and assisting State in developing a comprehensive information security program. State formally acknowledged weaknesses in its information security management and generally agreed with our recommendations. Senior State managers say that their commitment to improving information security has increased but that fully implementing our recommendations will require time and resources.

Department of Justice

In September 1997, the Department of Justice IG reported serious departmentwide computer-based control weaknesses that jeopardized a number of sensitive operations.[12] Access controls were weak over files supporting various operations at the Federal Bureau of Investigation, Drug Enforcement Administration, Immigration and Naturalization Service, and the U.S. Marshals Service. User passwords were not required to be changed, security software was not configured to prevent access by inactive users, system programmers had been inappropriately provided the ability to make numerous types of modifications to files that would allow them to circumvent security controls or assist others in such actions. Program change control procedures for system and application software were not formally documented or uniformly followed, increasing the risk that unauthorized software changes or unintentional errors could be made. Further, the IG reported that the department did not have a plan to recover primary systems, critical data processing applications, or key business processes in the event of a disaster. An underlying problem was that written security policies and procedures were outdated and did not define the roles and responsibilities of managers and others with security responsibilities. The Department of Justice management agreed with the findings and has stated that each departmental component will work with Justice's CIO to develop corrective actions.

[12]U.S. Department of Justice Annual Financial Statement for Fiscal Year 1996 (DOJ/OIG-97-24B, September 1997).

Other Federal Operations

Examples of risks at other agencies include the following:

- In May 1998, we reported that weak computer security practices at the Federal Aviation Administration (FAA) jeopardize flight safety.[13] FAA's air traffic control network is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that reside at, or are associated with, hundreds of facilities. All the critical areas included in our review—facilities physical security, operational systems information security, future systems modernization security, and management structure and policy implementation were ineffective. For example, in the physical security area, a March 1997 inspection of one facility that controls aircraft disclosed 13 physical security weaknesses, including unauthorized personnel being granted unescorted access to restricted areas. FAA is unaware of the weaknesses and vulnerabilities that may currently exist at other locations because the agency has not assessed the physical security controls at 187 facilities since 1993. When we met with FAA officials in late July 1998, they acknowledged that major improvements are needed in all areas of FAA's security program and discussed preliminary efforts to address most of our recommendations.
- In April 1997, the Department of Transportation's IG identified multiple security exposures in the Department's extended wide area network which connects hundreds of local area networks and 50,000 computer workstations that support operations throughout the department, including the Federal Aviation Administration, Federal Highway Administration, United States Coast Guard, Federal Railroad Administration, National Highway Safety Traffic Administration as well as DOT headquarters.[14]
- In April 1997, the Department of Housing and Urban Development's IG identified a variety of weaknesses that affected systems critical to supporting all facets of the department's operations, including providing (1) housing subsidies for low and moderate income families, (2) grants to states and communities, and (3) direct loans for construction and rehabilitation of housing projects.[15] In particular, weaknesses associated with an application that annually processed over $9 billion in disbursements increased the risk of over or underpayments to housing

[13]Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155 May 18, 1998).

[14]Report on the Department of Transportation Fiscal Year 1996 Consolidated Financial Statement (AD-OT-7-004, April 10, 1997).

[15]Audit of the U.S. Department of Housing and Urban Development's Fiscal Year 1996 Financial Statements (97-FO-177-0003, April 10, 1997).

authorities, inaccurate budget projections, and users maliciously entering unauthorized transactions for payments.

- In July 1997, the audit of the Department of Education's fiscal year 1996 and 1995 financial statements reported access control weaknesses in the Payment Management System, which controlled disbursements of over $28 billion annually. As a result, unauthorized users could potentially have accessed confidential data, changed data, made unauthorized payments, or disabled the system.[16]
- In April 1997, the Department of the Interior's IG reported[17] that the Bureau of Indian Affairs' had not implemented an effective system security program for the Bureau's major and sensitive mainframe applications, including the Land Records Information System and the Individual Indian Monies System, that processed approximately 2.5 million transactions weekly. In particular, the Bureau had inadequate (1) access controls over the mainframe computers, (2) software development and change controls, and (3) segregation of duties for the systems support functions, including data administration, data security, and quality assurance/testing. In addition, a service continuity plan had not been developed and the off-site storage facility was not secure or environmentally protected.
- In March 1997, the Department of Commerce Inspector General reported material weaknesses at several Commerce Bureaus. For example, the Economic Development Administration, which managed a $1 billion grant program in fiscal year 1997, did not adequately segregate programming responsibilities or adequately restrict access to its information systems. Inappropriately segregated duties can lead to implementation of unauthorized or inadequately tested programs. Further, unrestricted access can lead to accidental or intentional changes to program data.[18]

Recommended corrective actions have been provided to each of these agencies, and many have begun to implement them.

[16]U.S. Department of Education Fiscal Years 1996 and 1995 Financial Statements and Accompanying Notes, Price Waterhouse, LLP July 31, 1997.

[17]Audit Report on General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (Number 97-I-771, April 30, 1997).

[18]The U.S. Department of Commerce Consolidating Financial Statements Fiscal Year 1996 (Audit Report No FSD-9355-7-0001, March 1997) (attachment 1, Department of Commerce IG report, Economic Development Administration report, p. 5).

Although Nature of Risks Vary, Control Weaknesses Across Agencies Are Similar

Although the nature of agency operations and the related risks vary, there are striking similarities in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. In many cases, agencies have developed policies and begun to implement control techniques that could provide effective security. However, they have not yet done enough to ensure that these policies and controls remain effective on an ongoing basis. The following sections describe each of the six areas of general controls and the specific weaknesses that were most widespread at the agencies covered by our analysis.

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.

Despite the importance of this aspect of an information security program, we found that poor security planning and management was a widespread problem. Of 17 agencies where this aspect of security was reviewed, all had deficiencies. Many 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. Examples include the following.

- In August 1997, the IG at the Department of Health and Human Services reported that the Health Care Financing Agency had not reviewed internal controls or developed security plans for its computer center, telecommunications networks, or significant applications. Further, it did not have a consistent set of policies for overseeing the effectiveness of security at its contractor locations.[19]
- In July 1997, the Department of the Treasury IG reported that the Bureau of Alcohol, Tobacco and Firearms had not developed formal policies, standards, and procedures; had not established a formal program for

[19]Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1996 (A-17-96-00001, August 29, 1997).

security awareness and training; and had not identified all of its major applications.[20]

- In April 1997, we reported that the Internal Revenue Service needed to strengthen computer security management and that its approach to computer security was not effective in preventing serious and persistent computer security control weaknesses that exposed tax processing operations to the serious risk of disruption and taxpayer data to the risk of unauthorized use, modification, and destruction.[21]
- In May 1997, independent auditors recommended that the Office of Personnel Management develop security plans, identify system owners, and require periodic independent reviews of security controls.[22]
- In May 1996, we reported that the Department of Defense needed to establish a more comprehensive information systems security program. Specific weaknesses included (1) outdated and incomplete policies for detecting and reacting to computer attacks, (2) lack of awareness among computer users, and (3) inadequately trained system and network administrators.[23]

As a result of these types of deficiencies, agencies (1) were not fully aware of the information security risks to their operations, (2) had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable, (3) had a false sense of security because they were relying on controls that were not effective, and (4) could not make informed judgments as to whether they were spending too little or too much of their resources on security. Security program management is discussed in greater detail in chapter 3.

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 (1) require users to authenticate themselves through the use of secret passwords or

[20]Audit of the Bureau of Alcohol, Tobacco, and Firearms Fiscal Years 1996 and 1995 Financial Statements (OIG-97-094, July 9, 1997).

[21]IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997).

[22]Financial Statements, Fiscal Year 1996, U.S. Office of Personnel Management, Independent Auditors' Report (May 30, 1997).

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

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. Without adequate access controls, unauthorized individuals, including outside intruders or terminated employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users could unintentionally modify or delete data or execute changes that are outside of their span of authority.

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

Access control weaknesses were reported for all 23 of the agencies for which this area of controls was evaluated. Specific common problems included the following.

- Managers had not precisely identified access needs for individual users or groups of users. Instead, they had provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, for instance, a number of interconnected systems with very poorly implemented access controls were accessible from remote locations by anyone who had the telephone number for the supporting network. Because access controls associated with both the network and the systems were weak, an anonymous intruder could easily have dialed into the network, accessed any one of several systems, and committed any number of malicious actions, including reading, modifying, and deleting both data and other users' access rights and severely disrupting service. At another agency, 90 employees could change amounts available to grantees and contractors associated with an $8 billion grant program.

- Access was not appropriately authorized and documented. For example, at one agency, user access was verbally requested and approved and no related documentation was maintained.
- Users shared accounts and passwords or posted their passwords in plain view, making it impossible to trace specific transactions or modifications to an individual. Also, use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access control coverage. For example, at one agency location, any one of 17,000 system users could search, view, and print information in any of the other users' print files because access to temporary files holding users' output was not adequately restricted.
- User activity was not adequately monitored to deter and identify inappropriate actions, and when suspicious activity was noticed, it was often not investigated nor the perpetrator penalized. For example, records of user activity, referred to as audit logs, were either not maintained, not maintained in a useable format, or were too voluminous to be practical. As a result, it was either not possible or practical to review these logs to identify inappropriate actions and link any such actions to individual users. Such monitoring is especially important to prevent users with access to sensitive data from inappropriately browsing data that do not pertain to the work at hand and to identify activity indicating an intrusion into a network or system. However, tests showed that most attacks at this agency were not detected and reported.
- Access was not promptly terminated when users either left the agency or adjusted when their responsibilities no longer required them to have access to certain files. In addition, inactive user identifications were not routinely identified and deleted. As a result, contractors and former employees who were no longer associated with the agency, could still read, modify, copy, or delete data, and employees who changed positions within an agency had access to files that were not needed in their new positions. For example, at one location, automated controls were set to allow former employees access for 90 days after their employment had terminated.

To illustrate the risks associated with poor authentication and access controls, in recent years, we have begun to incorporate penetration testing into our audits of information security. Such tests involve attempting to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. Unfortunately, our auditors have been successful, in almost every test, in

readily gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purpose they had in mind.

Application Software Development and Change Controls

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

The effectiveness of software change controls is of particular concern as agencies design, test, and implement changes to ensure that their computer software will properly handle the year-2000 date change. As the end of the millennium approaches, agencies are under increasing pressure to ensure that their computers can distinguish between the year 1900 and the year 2000, since many use only the last two digits when identifying years. In an effort to accomplish these changes on time, agencies may be forced to speed up their software change process and increase their reliance on newly hired personnel or contractors. In such an environment, it will be especially important to ensure that software changes are properly tested and approved before they are implemented.

Weaknesses in software program change controls were identified for 14 of the 18 agencies where such controls were evaluated. The most common types of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, changes were made directly to software programs in operation rather than in a separate and controlled test environment, increasing the risk that

erroneous or unauthorized software would result in miscalculations of pension liability.

- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally-developed" unauthorized software programs was prevented or detected.
- Access to software program libraries was inadequately controlled. For example, at one agency, most system users—over 13,000 individuals—had the ability to modify application programs that processed millions of dollars in financial transactions. At another agency, approximately 16,000 users had unrestricted access to application programs, which allowed them to modify and delete programs and data.

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

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

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a

combination of physical and logical access controls and by effective supervisory review.

Segregation of duties was evaluated at 17 of the 24 agencies covered by our analysis. 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 providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation. Segregation of duty problems also were identified related to transaction processing. 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.

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

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate

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.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier in this section. 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.

Operating system software controls were covered in audits for only 9 of the 24 agencies included in our review. However, problems were identified for all 9 agencies, illustrating the importance of reviewing operating system controls. A common type of problem 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.

Service Continuity Controls

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

Although often referred to as disaster recovery plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasing of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location.

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

Service continuity controls were evaluated for 20 of the agencies included in our analysis. 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. For example, one agency had identified critical workloads and processing priorities that would need to be resumed and supported after a disruption but had not identified the specific software needed for users to perform their jobs. Such information could be difficult to compile in the confusion that would be likely after a major disruptive event.
- 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.

Conclusion

Important operations at every major federal agency are at some type of risk due to weak information security controls. There are many specific causes of these weaknesses, but many result from poor security program management and poor administration of available control techniques.

The audit reports cited in this chapter include numerous recommendations to individual agencies that address the specific weaknesses reported. For this reason, we are making no additional recommendations to these agencies in this report. However, our executive guide, Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), discusses the results of our recent study of information security best practices and outlines a number of principles and practices that could enable federal agencies to implement more

effective information security programs. Chapter 3 summarizes the principles outlined in the executive guide.

Need for Improved Security Program Planning and Management at Individual Agencies

Although auditors can provide periodic independent assessments of agency operations, ultimately it is agency management that is responsible for ensuring that internal controls, including information security controls, are appropriately selected and effectively implemented on an ongoing basis. In September 1996, we reported that an underlying cause of poor federal information security was that many agencies had not instituted a framework for proactively managing the information security risks associated with their operations.[1] Instead, there was a tendency to react to individual audit findings as they were reported, with little ongoing attention to the systemic causes of control weaknesses. Since then, as discussed in chapter 2, additional audits have identified the same underlying problem. Security program planning and management deficiencies were reported for 17 of the 24 agencies included in our analysis. In particular, agencies were not adequately assessing risks and monitoring control effectiveness.

To identify potential solutions to this problem, during 1997, we studied the security management practices of eight nonfederal organizations known for their superior security programs. 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 findings were initially published as an exposure draft in November 1997. Subsequently, they were published in May 1998 in an executive guide entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). The guide is generally consistent with OMB and NIST guidance on information security program management, and it has been endorsed by the CIO Council as a useful resource for agency managers. The guide's major points are summarized below.

Best Practices Provide a Framework for Improvement

Our study of information security management practices identified a fundamental set of management principles and 16 specific practices. Together, these principles and practices constitute a cycle of activity for managing risk.

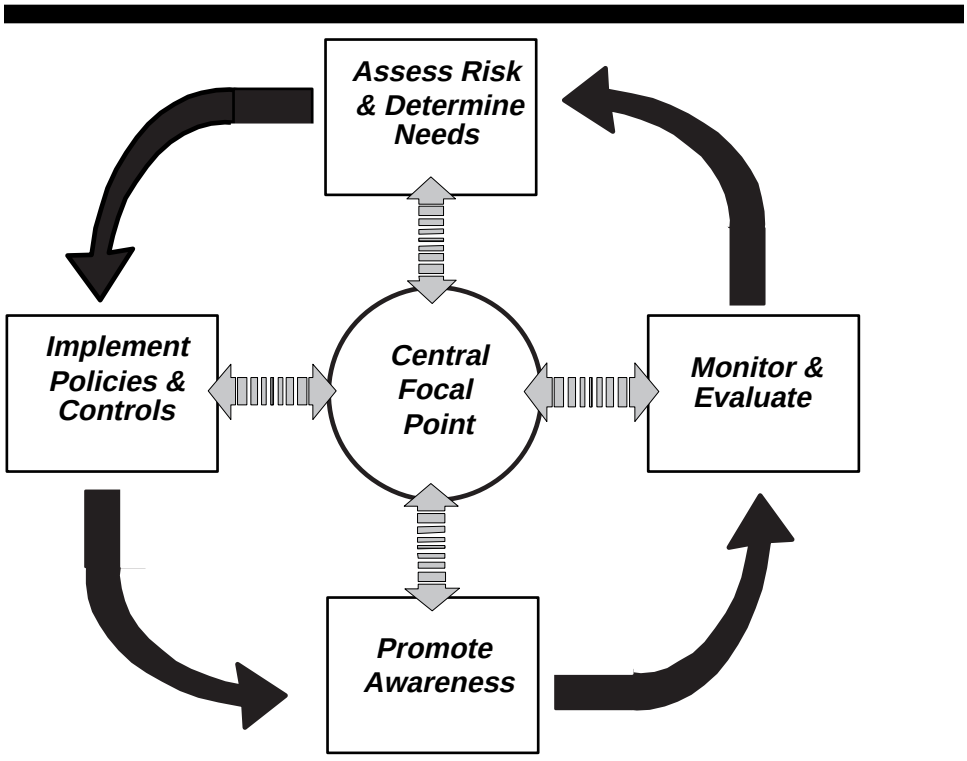
The Risk Management Cycle

The risk management cycle, as depicted in figure 3.1, begins with an assessment of risk and determination of needs, including selecting cost-effective policies and related controls. Once policies and controls are decided on, they must be implemented. Then, policies and controls, as

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

well as the risks that prompted their adoption, must be communicated to those responsible for complying with them. Finally, and perhaps most importantly, there must be procedures for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action. Also, our study found that a strong central security management 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. This cycle of activity, coordinated by a central focal point, can help ensure that existing controls are effective and that new, more advanced control techniques are prudently and effectively selected and implemented.

Figure 3.1: The Risk Management Cycle



The elements of the risk management cycle are not new. They have been described in various ways in OMB and NIST guidance and in various other guides on information security and internal controls. Nevertheless, as

basic as these principles are, audits continue to show that many federal agencies have not implemented this cycle of activity.

One possible cause for this deficiency is that some senior agency officials, like many private sector executives, may be just beginning to realize how critical their information resources are to their program operations and may not fully understand that security weaknesses present formidable risks to mission-related operations. Another reason is that maintaining adequate information security can be difficult. The complicated and technical nature of many of the risks and controls requires that organizations adopt more defined processes than are needed to manage other types of internal controls. These defined processes are needed to ensure that personnel with the right mix of expertise are involved in risk management decisions; that all pertinent factors are considered; that the effectiveness of controls, especially technical controls, is reliably evaluated; and that the results of these evaluations and their potential effects on critical operations are clearly reported to senior officials.

Within this basic risk management cycle, we identified 16 practices that were key to the effectiveness of an information security program. A brief description of these practices, organized according to the five elements of the risk management cycle, follows. A more detailed description accompanied by case examples can be found in our executive guide.

Assess Risk and Determine Needs

Practice 1: Recognize Information Resources as Essential Organizational Assets

Organizations that have become heavily dependent on computers, electronic data, and telecommunications to conduct their activities must recognize that these information resources are critical assets, essential to supporting business operations. Information protection should be viewed as an integral element of operational management and strategic planning. In particular, senior executives must understand the importance of data and systems and be willing to devote an appropriate level of resources to protecting these assets.

Practice 2: Develop Practical Risk Assessments That Link Security to Business Needs

Security needs should be based on risk, and this requires some type of risk assessment. Various methods can be used, from relatively informal discussions to complex analyses. Key success factors are that risk assessments

- be required and involve defined minimum procedures;
- involve a mix of individuals with knowledge of business operations and technical aspects of the organization's systems;
- rank, but not necessarily precisely quantify, risks;
- require sign-off by business managers indicating agreement with risk reduction decisions and acceptance of the residual risk; and
- result in documentation that is provided to more senior officials and internal auditors, so that participants can be held accountable for their decisions.

Practice 3: Hold Program and Business Managers Accountable

Primary responsibility for managing risk should rest with business or program managers because they are in the best position to determine what the business impact of a loss of integrity, confidentiality, or availability of information resources would be. The security specialists, on the other hand, should play more of an educational and advisory role. However, they should not hesitate to elevate discussions to higher levels if they believe that inappropriate risk management decisions are being made.

Practice 4: Manage Risk on a Continuing Basis

Risk must be continuously reassessed because the factors that affect risk —threats, technology, known vulnerabilities, and the sensitivity of the operations being supported—frequently change.

Establish a Central Management Focal Point

Practice 5: Designate a Central Group to Carry Out Key Activities

Central security management groups can ensure that the various elements of the risk management cycle are implemented. They can also serve as a conduit for communicating information across organizational lines and from outside sources.

Practice 6: Provide the Central Group Ready and Independent Access to Senior Executives

Regardless of their organizational position, an organization's central security manager must feel that he or she can comfortably raise issues to higher levels. Independent access to senior executives allows senior security managers to provide an objective assessment of security needs and gives them the clout to be effective throughout their organizations.

Practice 7: Designate Dedicated Funding and Staff

Central groups should have defined budgets that allow them to plan and set goals. However, they may also rely on a network of subordinate security specialists who work in other organizational units.

Practice 8: Enhance Staff Professionalism and Technical Skills	Develop security managers into a cadre of respected specialists. Technical training and professional certification should be encouraged and kept current.

Implement Appropriate Policies and Related Controls

Practice 9: Link Policies to Business Risks	Policies and the controls to implement policies should flow directly from risk assessments and, thus, be linked to business risks. Also, as risk factors change, policies and controls should be updated.
Practice 10: Distinguish Between Policies and Guidelines	Distinguishing between policies and guidelines provides flexibility for individual business units. However, high-risk operations are likely to require a more detailed set of mandatory policies and standards.
Practice 11: Support Policies Through the Central Security Group	Central groups can promote consistency in policy implementation by developing the related written documents, based on input from business managers, attorneys, and others, and by serving as the organizational focal point for policy questions.

Promote Awareness

Practice 12: Continually Educate Users and Others on Risks and Related Policies	Awareness of both risks and policies should be vigorously promoted so that users understand the importance of complying with policies and controls. In particular, sensitizing employees and other users to risks can make users (1) think twice before revealing sensitive data and (2) more likely to notice and report suspicious activity.
Practice 13: Use Attention-Getting and User-Friendly Techniques	Various promotion techniques, such as intranet websites, awareness days, and posters can keep security in the forefront of users' minds. Two effective techniques are customized briefings to individual business units and videos featuring top organization executives promoting security as everyone's responsibility.

Monitor and Evaluate Policy and Control Effectiveness

Practice 14: Monitor Factors That Affect Risk and Indicate Security Effectiveness

Managers should develop procedures for periodically evaluating the effectiveness of their information security programs, paying closest attention to the controls associated with the most critical operations. Monitoring and evaluation efforts should focus primarily on (1) determining if controls are operating as intended and (2) evaluating the effectiveness of the security program in communicating policies, raising awareness levels, and reducing incidents. Testing controls, including penetration testing, is an effective way to determine if policies and controls are operating effectively. Other types of monitoring and evaluation activities include periodic reports on compliance with various policies, the number of inquiries from users, and the number and nature of security incidents reported.

Practice 15: Use Results to Direct Future Efforts and Hold Managers Accountable

The full benefits of monitoring are not achieved unless results are reported to officials who can take any actions needed to improve the security program. Such action can include (1) reassessing previously identified risks, (2) identifying new problem areas, (3) reassessing the appropriateness of existing controls and security-related activities, (4) identifying the need for new controls, (5) redirecting subsequent monitoring efforts, and (6) holding managers accountable for compliance. Effecting change and holding managers accountable generally requires involvement of an organization's most senior executives.

Practice 16: Be Alert to New Monitoring Tools and Techniques

Because new technology is being introduced at a fast pace, with related security controls often lagging behind, security specialists must keep abreast of information on new risks and control techniques through professional organizations and literature.

Improved Security Depends on Broader Improvements to Information Technology Management

The risk management activities described in our executive guide and summarized above are likely to be most successful if implemented in the context of broader improvements to federal information technology management. Over the last few years, the Congress has enacted legislation that is prompting landmark reforms in this broader area. In particular, the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996 emphasize the need for agencies to apply information resources to effectively support agency missions and delivery of services to the public.

These laws stress the importance of involving senior executives in information management decisions, appointing senior-level chief information officers, and using performance measures to assess the contribution of technology in achieving mission results. Both specify security as an aspect of information management that must be addressed. These broader information management improvements are apt to improve security management because they prompt senior agency officials to take a more active role in managing their organizations' use of information technology. Further, agencies may find this environment of reform conducive to rethinking their security programs and considering new practices.

Conclusion

Although existing federal guidance outlines basic security planning and management requirements, many, if not most, of the reported weaknesses in agency information security controls can be traced to poor performance in this area. Good management is essential to ensure that relied-upon controls are working effectively on a continuous basis. It is also important to help ensure that agencies promptly identify emerging risks and take full advantage of more sophisticated security controls as they become available. Our executive guide, which outlines the risk management practices employed by leading organizations, provides a framework of solutions that supplement existing federal guidance and can assist agencies in strengthening their management of this critical area.

Centrally Directed Improvement Efforts Have Increased, but Most Have Not Progressed Beyond Planning Stage

Several new governmentwide efforts to improve federal information security have been initiated since we last reported on this topic in September 1996, such as the recent issuance of Presidential Decision Directive (PDD) 63 on critical infrastructure protection. Most of these efforts, however, had only recently been started and had not progressed far beyond the planning stages at the close of our review. In addition, while these efforts address some important information security problems, such as inadequate risk awareness and incident reporting capabilities, none provides a comprehensive strategy for adequate monitoring and oversight of agency performance in this area.

Federal agencies are primarily responsible for protecting their respective information resources, but governmentwide leadership, coordination, and oversight are important to (1) ensure that federal executives understand the risks to their operations, (2) monitor agency performance in mitigating these risks, (3) ensure implementation of needed improvements, and (4) 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.

Since September 1996, OMB has continued to review selected agency system-related projects and provide input through various federal task forces and working groups. These efforts were supplemented in late 1997 when the CIO Council, under OMB's leadership, designated information security as one of six priority areas and established a Security Committee. The Committee, in turn, has developed a preliminary plan and taken several actions primarily related to promoting awareness, planning for improving agency access to incident response services, and establishing links with other federal entities involved in security issues. However, neither OMB nor the Council has developed a comprehensive strategy for ensuring that agency security programs are effective.

More recently, in May 1998, PDD 63 was issued, which established several 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. This directive specified several requirements related to evaluating and coordinating federal agency information security practices. However, at the close of our review in early August 1998, it was not clear how and when these new requirements would be implemented and how

they would be coordinated with existing requirements and with efforts underway at other federal entities.

Previous Recommendations Urged More Active Oversight

In 1996, we reported that, although OMB had improved federal guidance pertaining to information security, its oversight efforts were uneven, and it generally did not proactively attempt to identify and promote resolution of fundamental security program weaknesses that were likely to be at the root of reported deficiencies at individual agencies. Our report recommended that OMB

- take advantage of the wide range of information currently reported in financial statement audit reports and agency self-assessments to monitor agency compliance with OMB's guidance and the effectiveness of agency information security programs, and
- implement a program for increasing its program examiners' understanding of information security management issues so that they can more readily identify and understand the implications of information security weaknesses on agency programs.

We also recommended that OMB promote the CIO Council's (1) adoption of information security as one of its top priorities and (2) development of a strategic plan for increasing awareness of the importance of information security, especially among senior agency executives, and improving information security program management governmentwide. We suggested that the CIO Council's strategic plan include plans for

- developing information on the existing security risks associated with nonclassified systems currently in use,
- developing information on the risks associated with evolving practices, such as Internet use,
- identifying best practices regarding information security programs so that they can be adopted by federal agencies,
- establishing a program for reviewing the adequacy of individual agency information security programs,
- ensuring adequate review coverage of agency information security practices by considering the scope of various types of audits and reviews performed and acting to address any identified gaps in coverage,
- developing or identifying training and certification programs that can be shared among agencies, and
- identifying proven security tools and techniques.

CIO Council Plans Focus on Solving Selected Crosscutting Problems

The CIO Council has begun to lay the groundwork for improvements in several areas, but has not developed a comprehensive strategy that identifies the most critical issues affecting federal information security and includes long-term goals and objectives, including annual performance goals. During 1997, the Council discussed various critical information management issues, and in late 1997, formally declared information security as one of six priority areas that will guide the Council's activities. The stated goal for this area is to "ensure implementation of security practices within the Federal Government that gain public confidence and protect Government service, privacy, and sensitive and national security information." Two other priority areas—defining an interoperable architecture and improving information technology workforce skills—may also support security improvements. An interoperable federal computer systems architecture will make it easier to implement and manage security controls, and improving technical workforce skills will help provide expertise needed to select and properly implement technical controls.

To guide activities associated with its information security goal, the Council established the Security Committee, also in late 1997. Since then, the Committee has taken some steps to coordinate its plans with related activities at other federal entities and address some of the most prominent governmentwide problems associated with information security, such as insufficient awareness of risks, inadequate technical training, and poor incident response capabilities. These projects have been conducted during monthly meetings and by part-time efforts of individual committee members between meetings. Accomplishments as of August 1998 are described below.

Preliminary Strategic Plan Developed

During late 1997, the Security Committee developed a preliminary strategic plan, which was incorporated into a larger strategic information technology management plan developed jointly by OMB and the CIO Council and issued in January 1998.[1] The information security segment of the plan includes three general objectives: promote awareness and training, identify best practices, and address technology and resource issues. Under each of these objectives, three or four specific activities and related milestones are briefly identified. Committee members told us that they expect to expand on this initial plan as the year progresses.

[1]The Paperwork Reduction Act requires OMB to annually submit a governmentwide information technology plan to the Congress. The 1998 plan is the first such plan jointly prepared by OMB and the CIO Council.

Expansion of the plan is important to help ensure that the many facets of this problem are identified, prioritized, and addressed efficiently and effectively. Ideally, such a plan would identify the many policy, technical, legal, and human resource issues that affect federal information security and describe the various roles and activities of other federal entities involved in improving the protection of unclassified federal data. Such entities include, but are not limited to, NIST, the National Security Agency, and the Government Information Technology Services Board. A description of the information security-related activities of OMB's Office of Information and Regulatory Affairs, Office of Federal Financial Management, and program examiners also would be useful. Further, the plan could include long-term goals and objectives, including time frames, priorities, and expected accomplishments, and annual performance goals.

For example, to better coordinate agency activities, increase efficiency, and build on existing expertise, the plan could provide for identifying and sharing individual agency solutions to common challenges, such as incident handling, investigations, contingency planning, security plan development, virus protection, security awareness, and system architecture design. Related efforts could include, for each functional area,

- designating an individual to serve as a focal point;
- developing a consolidated e-mail directory for key agency personnel;
- identifying useful web sites and evaluation tools;
- publicizing software and training aids and opportunities; and
- reviewing, filtering, and distributing notices and advisories on software vulnerabilities, such as those issued by Carnegie-Mellon University's Computer Emergency Response Team.

In addition to coordinating and optimizing the value of agency efforts, such a plan could help inform agency managers about their information security responsibilities, maximize the value of audit results, and facilitate administration and Congressional oversight. Further, it could provide support for the governmentwide performance plan that OMB is required to include in the president's annual budget submission to the Congress under the Government Performance and Results Act. The first governmentwide performance plan and related "priority management objectives" were published in early 1998 as part of the President's Fiscal Year 1999 Budget. However, that plan provided few details on the administration's strategy for addressing widespread deficiencies in federal information security.

Efforts to Facilitate Projects Sponsored by Others

The Security Committee has established links with other federal entities with information security responsibilities, including NIST and the National Security Agency; requested briefings on other federally sponsored information security efforts; and acted to support and facilitate these efforts. For example, in late 1997 and early 1998, the Committee explored ways to gain broader federal agency participation in FedCIRC, a program initiated by NIST in 1996 to provide agencies a means of responding to computer security incidents. OMB Circular A-130, Appendix III, requires agencies to have a capability to (1) help users when a security incident, such as a suspected system intrusion, occurs, (2) share information on common vulnerabilities and threats, and (3) assist in pursuing appropriate legal action. In May 1998, the Council took action on the FedCIRC issue by endorsing the Security Committee's recommendation to shift sponsorship of FedCIRC to GSA and to change the funding mechanism. As of August 1998, the Council was developing detailed arrangements in anticipation of implementing the change at the start of fiscal year 1999.

Other briefing topics at Security Committee meetings have included our study of information security management best practices, which is discussed in chapter 3, and the "Information Security Countermeasures Assessment Project," sponsored by the Air Force Research Laboratory. The latter is an effort to develop a better understanding of the effectiveness of administrative and technical measures for preventing security incidents.

Security Awareness Seminar

In February 1998, the Security Committee arranged for and held a security awareness seminar to brief federal officials on information security risks. Speakers included representatives from the National Security Agency, NIST, and private sector organizations who described the latest challenges to maintaining adequate security. The seminar was attended by about 80 individuals—primarily agency CIO and federal agency information security officers. Comments from seminar attendees indicated that the program was a success and that more such programs addressing an expanded variety of topics would be welcome.

The results of our recent study of information security management practices indicate that it would be valuable to expand the reach of such awareness seminars beyond agency CIO offices to a broader audience of senior program executives. If program officials have a more thorough understanding of the information security risks to their operations and assets, they will be more likely to (1) encourage their staff to comply with

security requirements, (2) devote resources for security, and (3) make prudent decisions regarding the appropriate levels of protection needed.

Oversight of Agencies Remains Limited

A major aspect of our previous recommendations that is not being addressed by either OMB or the CIO Council is establishing a more structured program for ensuring that agency security programs are adequately evaluated and the results used to measure performance and prompt improvement. Minimum requirements for agency security programs are outlined in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Updated in February 1996, Appendix III requires agencies to assign responsibility for security, develop a system security plan, screen and train individual users, assess risk, plan for disasters and contingencies, and periodically review their security safeguards. It also requires agencies to clearly define responsibilities and expected behavior for all individuals with access to automated systems and to implement security incident response and reporting capabilities.

Central oversight of the effectiveness of agency security programs is important because audit results indicate that agencies are not adequately identifying and addressing security weaknesses on their own. One resource for such oversight is the large body of audit evidence that has become available in the last few years, primarily due to reviews of computer security controls performed as part of financial statement audits. Although, as discussed in chapter 2, comprehensive audits of computer security are not yet being performed at all agencies, analyses of these audit results and related reports could provide a starting point for measuring progress. The results can also be useful in identifying continuing problem areas and encouraging agency managers to take a more proactive role in identifying and addressing weaknesses themselves—before the weaknesses are discovered and reported by auditors.

OMB's Oversight Efforts Focus on Individual Issues and Projects

OMB's program examiners may consider information security during their broader review of an agency's mission-related programs, generally, as part of their review of agency information technology investment plans. Program examiners are assisted in this area by policy analysts in OMB's Information Policy and Technology Branch. In addition to their own specialized expertise, these policy analysts keep abreast of governmentwide information security issues by interacting with other

federal entities such as the Federal Computer Security Managers Forum, the National Security Telecommunications and Information Systems Security Committee, the Security Policy Board, and the National Security Telecommunications Advisory Committee.

In 1996, we reported that few of the program examiners had significant experience or expertise in dealing with information systems or related security issues and most did not consider the effectiveness of an agency's overall information security program. For this reason, in our September 1996 report, we recommended that OMB implement a program for increasing its program examiners' understanding of information security management issues and of the related audit results that were available to them.

Since then, officials in OMB's Information Policy and Technology Branch say that they have provided two specialized security training sessions to program examiners and have continued to advise them on various security-related issues, such as the adequacy of system security plans, authentication, encryption, privacy of data and databases, and Internet and World Wide Web use. Agency projects cited as receiving attention pertaining to information security since early 1997 include (1) DOD's Defense Messaging System, (2) the FBI's National Crime Information Center information sharing initiative, (3) encryption of online services at the Departments of Education and the Interior and the Office of Personnel Management, and (4) critical infrastructure protection issues at the Federal Aviation Administration and the Departments of Energy and Defense.

A More Comprehensive and Structured Assessment Program Would Provide Benefits

While OMB's policy analysts and program examiners can provide valuable oversight of specific issues and projects, in light of the continuing reports of serious deficiencies, a more structured approach for measuring broader compliance with Circular A-130, Appendix III, and the effectiveness of agency security programs is needed. To be effective, such an approach must include comprehensive evaluations and tests of agency security programs at major agencies and reports at regular intervals that show improvements and deteriorations in program effectiveness.

Much could be learned by analyzing the results that are already available from financial statement audits, as discussed in chapter 2. Also, agency-initiated assessments, required by both OMB Circular A-130, Appendix III, and FMFIA, can be a source of evaluation results. Periodic

evaluations initiated by agency management are an essential step in helping determine whether controls are effective, which is an essential aspect of managing risk, as discussed in chapter 3. However, recent audits have identified numerous serious information security weaknesses that have apparently not been identified by agency managers and have not been reported in annual reports to the President and the Congress, as required by FMFIA. As a result, these reports are of limited value for oversight and, more importantly, agencies do not have the information they need to manage their information security risks.

To assist agencies in reviewing their computer-based controls and supplement audit information that is already available, OMB or the CIO Council could establish an independent cadre of experts to review critical areas of agency operations that are not being adequately evaluated. Such a cadre of experts could be created by drawing on the resources of many federal agencies, as we suggested in our September 1996 report, or a specialized unit could be established at an agency that already has a relatively high degree of expertise, such as NIST or the National Security Agency.

Regardless of how and by whom evaluations are conducted, results could be used to measure agency performance, identify recurring or longstanding problems, and identify gaps in audit coverage. For example, annual summary reports could be developed to show (1) the most commonly reported types of problems and (2) agencies where the same information security weaknesses were identified for more than 1 year. More refined performance indicators could distinguish between weaknesses classified as "material weaknesses" and those considered "reportable conditions," which are less serious than material weaknesses. These are standard classifications used in financial statement audit reports. OMB and the CIO Council could work with agency IGs, through the President's Council on Integrity and Efficiency, to develop other performance indicators. Such an annual "report card" could highlight improvements in agency performance as well as provide agencies an additional incentive to avoid being designated as an organization with long-standing information security problems.

PDD 63 Supplements Existing Requirements From a National Security Perspective

PDD 63 provides for additional central oversight of agency practices by the National Security Council in the Executive Office of the President. However, at the close of our review in August 1998, it was too early to determine how these provisions would be implemented, how effective they would be, and how they would be coordinated with ongoing efforts by the CIO Council and others.

In its October 1997 report, Critical Foundations: Protecting America's Infrastructures, the President's Commission on Critical Infrastructure Protection recognized the need for improved oversight of agency security practices and recommended assigning responsibility for oversight of federal systems security to a proposed Office of National Infrastructure Assurance within the National Security Council. As envisioned by the Commission, this Office would be given "overall program responsibility for infrastructure assurance matters, including policy implementation, strategy development, federal interagency coordination, and liaison with state and local governments and the private sector."

On May 22, 1998, PDD 63 established such an entity under the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, who is to report to the President through the Assistant to the President for National Security Affairs. This new entity, termed the Critical Infrastructure Coordination Group, is to be supported by a newly created Critical Infrastructure Assurance Office within the Department of Commerce.

The PDD addresses a range of national infrastructure protection issues and includes several provisions intended to ensure that critical federal computer, or "cyber-based," systems are protected from attacks by our nation's enemies. Specifically, it states that "the Federal 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. Although details are not provided, 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. The Critical Infrastructure Coordination Group is then to sponsor an "expert review process" for those plans. 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.

Several of these provisions appear to overlap with existing requirements prescribed in the Paperwork Reduction Act of 1980, OMB Circular A-130, Appendix III, the Computer Security Act, the Clinger-Cohen Act, and the Federal Managers' Financial Integrity Act. In addition, some of PDD 63's objectives are similar to objectives being addressed by other federal entities, such as development of the FedCIRC program by NIST and the CIO Council. The relationship among these requirements and existing efforts had not been clarified at the conclusion of our review.

Conclusion

Since September 1996, the need for improved federal information security has received increased visibility and attention. However, central oversight has remained limited and a comprehensive strategy has not been developed. As a result, many aspects of the recommendations we made in September 1996 are still applicable. The CIO Council's efforts during late 1997 and the first half of 1998, as well as issuance of PDD 63 in May 1998, indicate that senior federal officials are increasingly concerned about information security risks, both to federal operations as well as to privately-controlled national infrastructures, and are now moving to address these concerns. Coordinated efforts throughout the federal community, as envisioned by PDD 63, will be needed to successfully accomplish the objectives of these efforts and substantively improve federal information security. It is especially important that a governmentwide strategy be developed that clearly defines and coordinates the roles of new and existing federal entities in order to avoid inappropriate duplication of effort and ensure governmentwide cooperation and support.

Recommendation

Accordingly, we recommend that the Director of the Office of Management and Budget and the Assistant to the President for National

Security Affairs ensure that the various existing and newly initiated efforts to improve federal information security are coordinated under a comprehensive strategy. 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 federal 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.

Agency Comments and Our Evaluation

In commenting on a draft of this report, OMB's Acting Deputy Director for Management stated that OMB and the CIO Council, working with the National Security Council, have developed a plan to address the PDD 63 provision that the federal government serve as a model for critical infrastructure protection and to coordinate the new requirements of the PDD with the existing requirements of the various laws pertaining to federal information security. The comments further 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. Also described are plans for a CIO Council-sponsored interagency security assist team that will review agency security programs. Regarding our conclusion that many aspects of the recommendations in our September 1996 report are still applicable, OMB reiterated its concern that the 1996 report's "overemphasis on OMB's role could distract program managers in the Federal agencies from their primary responsibility for assuring information security."

OMB's comments indicate that it, the CIO Council, and the National Security Council are moving to coordinate their responsibilities and beginning to develop the comprehensive strategy that is needed. Based on the description provided, the plans being developed include several key elements, most notably a means of evaluating agency performance. These plans were still being finalized at the close of our work and were not yet available for our review. Accordingly, we are not able to comment on their content, scope, and detail, or whether they will be effective in improving federal information security.

Regarding OMB's concern that we have overemphasized its role, we agree that agency managers are primarily responsible for the security of their operations. Increased attention and support from central oversight, if done effectively, should not distract agencies from their responsibilities in this area. On the contrary, active oversight of agency performance is more likely to have the effect of emphasizing the agency managers' accountability and providing more visibility for agencies that are achieving their information assurance goals as well as those that are falling short.

GAO Reports on Information Security Issued Since March 1996

Note: This list does not include products for which distribution was limited to official use because the products contained sensitive information.

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

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998).

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

U.S. Government Financial Statements: Results of GAO's Fiscal Year 1997 Audit (GAO/T-AIMD-98-128, April 1, 1998).

Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997).

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997).

Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-89, August 29, 1997).

Small Business Administration: Better Planning and Controls Needed for Information Systems (GAO/AIMD-97-94, June 27, 1997).

Social Security Administration: Internet Access to Personal Earnings and Benefits Information (GAO/T-AIMD/HEHS-97-123, May 6, 1997).

Budget Process: Comments on S.261—Biennial Budgeting and Appropriations Act (GAO/T-AIMD-97-84, April 23, 1997).

IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified (GAO/T-AIMD-97-82, April 15, 1997).

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/T-AIMD-97-76, April 10, 1997).

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997).

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

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

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements (GAO/AIMD-96-101, July 11, 1996).

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996).

Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996).

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

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996).

Security Weaknesses at IRS' Cyberfile Data Center (GAO/AIMD-96-85R, May 9, 1996).

Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome To Achieve Success (GAO/T-AIMD-96-75, March 26, 1996).

Agency Reports Issued Since September 1996 That Identify Information Security Weaknesses

Department of Health and Human Services Accountability Report: Fiscal Year 1997 (April 1998).

Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1997 (A-17-97-00097, April 24, 1998).

Report on the Department of Health and Human Services Consolidated Financial Statements for Fiscal Year 1997 (A-17-98-00001, April 1, 1998).

Department of the Treasury's Inspector General Report: Report on the U.S. Customs Service's Fiscal Years 1997 and 1996 Financial Statements (OIG-98-050, March 5, 1998).

Audit of the Extent to Which USAID's Financial Management System Meets Requirements Identified in the Federal Financial Management Improvement Act of 1996 (OIG-A-000-98-003-P, March 2, 1998).

Report on USAID's Financial Statements, Internal Controls, and Compliance for Fiscal Years 1997 and 1996 (OIG-0-000-98-001-F, March 2, 1998).

EPA's Fiscal Year 1997 and 1996 Financial Statements Audit Report (E1AML7-20-7008-8100058, March 2, 1998).

NASA Data Center General Controls, Johnson Space Center (IG-98-005, January 29, 1998).

Federal Managers' Financial Integrity Act Report, Fiscal Year 1997 (USAID, December 31, 1997).

EPA 1997 Integrity Act Report to the President and Congress (EPA-205-R-98-002, December 19, 1997).

Social Security Accountability Report for Fiscal Year 1997, (SSA Pub. No. 31-231, November 1997).

General and Application Controls Over the Mechanization of Contract Administration Services System (DODIG, Report Number 98-007, October 9, 1997).

Audit of USAID's Compliance with Federal Computer Security Requirements (OIG-A-000-97-008-P, September 30, 1997).

Audit of the Status of USAID's New Management System (NMS) (OIG-A-000-97-010-P, September 30, 1997).

Audit of the Internal Controls for the Operational New Management System (OIG-A-000-97-009-P, September 30, 1997).

NASA Data Center General Controls, Marshall Space Flight Center (IG-97-039, September 30, 1997).

Evaluation of the Social Security Administration's Back-up and Recovery Testing of Its Automated Systems (SSA/OIG-A-13-97-12014, September 24, 1997).

U.S. Department of Justice Annual Financial Statement for Fiscal Year 1996 (DOJ/OIG-97-24B, September 1997).

Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1996 (A-17-96-0001, August 29, 1997).

NASA Data Center Facility, Langley Research Center (IG-97-035, August 28, 1997).

U.S. Department of Education Fiscal Years 1996 and 1995 Financial Statements and Accompanying Notes (Price Waterhouse, LLP, July 31, 1997).

Physical Security at Ames Research Center's NAS Facility (IG-97-030, July 18, 1997).

Audit of USAID's Efforts to Resolve the Year 2000 Problem (OIG-A-000-97-005-P, July 11, 1997).

Department of the Treasury's Inspector General Report: Audit of the Bureau of Alcohol, Tobacco and Firearms Fiscal Years 1996 and 1995 Financial Statements (OIG-97-094, July 9, 1997).

The Royalty Management Program's Automated Information Systems, Minerals Management Service (DOI/OIG-97-I-1042, July 1997).

Review of Physical Security at the Social Security Administration's National Computer Center (SSA/OIG-A-13-96-11046, June 26, 1997).

Audit of OPM's Benefit Programs Fiscal Year 1996 Financial Statements - Management Letter (Transmitted to OPM's OIG on June 20, 1997).

Review of the Back-up and Recovery Procedures at the National Computer Center (SSA/OIG-A-13-96-11052, June 19, 1997).

Audit of OPM's Benefit Programs Fiscal Year 1996 Financial Statements (Transmitted to the Director, OPM, on June 17, 1997).

General Services Administration, Fiscal Year 1996 Management Letter Comments and Suggestions for Consideration (OIG-A62709, June 10, 1997).

Audit of Security Controls at the Hines Benefits Delivery Center, Department of Veterans Affairs, Office of Inspector General (Report Number 7D2-G07-062, May 13, 1997).

Audit of SBA's FY 1996 Financial Statements - Management Letter (SBA/OIG-7-6-H-006-015, April 29, 1997).

Audit of the U.S. Department of Housing and Urban Development's Fiscal Year 1996 Financial Statements (Case Number 97-FO-177-0003, April 10, 1997).

Report on the Department of Transportation Fiscal Year 1996 Consolidated Financial Statement (Report Number AD-OT-7-004, April 10, 1997).

Federal Emergency Management Agency Management Letter for the Year Ended September 30, 1996 (April 4, 1997).

General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (DOI/OIG-97-I-771, April 1997).

Department of the Treasury's Inspector General Report: Report on the U.S. Customs Service's Fiscal Years 1996 and 1995 Financial Statements (OIG-97-054, March 31, 1997).

NSF's Fiscal Year 1996 Management Letter Report (OIG-97-2110, March 31, 1997).

Review of CA-TOP SECRET Access Control Software (SSA/OIG-A-13-95-00606, March 18, 1997).

Department of Commerce's Consolidating Financial Statements for Fiscal Year 1996 (OIG-FSD-9355-7-0001, March 1, 1997).

Department of Commerce Economic Development Administration Financial Statements for Fiscal Year 1996 (OIG-FSC-8837-7-0001, March 1, 1997).

Department of Commerce International Trade Administration Financial Statements for Fiscal Year 1996 (OIG-FSC-8838-7-0001, March 1, 1997).

Department of Commerce National Oceanic and Atmospheric Administration Financial Statements for Fiscal Year 1996 (OIG-FSC-8841-7-0001, March 1, 1997).

Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation (DOI/OIG-97-I-683, March 1997).

U.S. Environmental Protection Agency FY 1996 Audited Financial Statements (March 1997).

Audit of SBA's FY 1996 Financial Statements (SBA/OIG-7-6-H-006-010, February 28, 1997).

Auditor's Reports on NSF's Fiscal Year 1996 Financial Statements, (Transmitted to the Chairman, NSF, on February 28, 1997).

U.S. Department of Labor Consolidated Financial Statement Audit for Fiscal Years 1995 and 1996 (DOL/OIG-12-97-005-13-001, February 28, 1997).

Reports on USAID's Financial Statements, Internal Controls, and Compliance for Fiscal Year 1996 (OIG-0-000-97-001-C, February 24, 1997).

Department of Veterans Affairs Annual Accountability Report for Fiscal Year 1996 (February 14, 1997).

U.S. Department of Energy Consolidated Financial Statements for Fiscal Year 1996 (February 1997).

Management Letter to the Administrator of NASA (January 31, 1997).

Secretary's Annual Statement and Report, Federal Managers' Financial Integrity Act, U.S. Department of the Treasury 1996 (December 30, 1996).

Report on Applying Agreed-Upon Procedures to the Internal Controls over the Federal Financial System, Fiscal Year Ended September 30, 1996 (NRC/OIG, November 25, 1996).

General Control Environment of the Federal Financial System at the Reston General Purpose Computer Center, U. S. Geological Survey (DOI/OIG-97-I-98, October 1996).

Interim Report on the Status of USAID's New Management System (OIG-A-000-96-001-S, September 27, 1996).

Department of Health and Human Services Accountability Report: Fiscal Year 1996.

Department of State Consolidated Financial Statements for Fiscal Year 1996.

Financial Statements Fiscal Year 1996, Office of Personnel Management.

National Aeronautics and Space Administration Fiscal Year 1996 Accountability Report.

Comments From the Office of Management and Budget

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 14, 1998

The Honorable Gene L. Dodaro
Assistant Comptroller General
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro:

Thank you for the opportunity to comment on your draft report entitled, Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92). The report's principal findings highlight many of the security challenges that are facing Federal agencies and other organizations as they increasingly rely on interconnected information systems for the conduct of agency business. The Office of Management and Budget (OMB) and the CIO Council have recognized these challenges, and, as the report acknowledges, have undertaken a number of initiatives to address them. The draft report also highlights the requirements of Presidential Decision Directive 63 which requires, among other things, that the Federal government serve as a model for critical infrastructure protection.

OMB and the CIO Council, working with the National Security Council, have developed a plan to address that charge and coordinate the new requirements of the PDD with the existing requirements of the Computer Security Act, Paperwork Reduction Act, and Clinger-Cohen Act. Our plan, which is integrated with the CIO Council Security Committee's strategic 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 to assure program improvement and effectiveness; and, 3) set in motion a process of continued maintenance. Coordination of these efforts will come primarily from the CIO Council and the President's Management Council, both co-chaired by OMB.

As part of this process, the CIO Council will sponsor an inter-agency security assist team that will perform independent and confidential reviews of agency security programs. As agency needs dictate, these reviews will include top-level program reviews for conformance to OMB Circular A-130, Appendix III and GAO's executive guide, "Information Security Management: Learning from Leading Organizations," and system-specific reviews to evaluate conformance with the Computer Security Handbook issued by the National Institute of Standards and Technology . Each review will also include selective system interdependency analysis and penetration testing. As GAO has found, among the chief benefits of penetration testing is the way it vividly demonstrates to agency managers the inadequacies of seemingly secure systems and programs.

The greatest challenge to enhancing information security programs and developing a workable infrastructure protection program is to ensure that protection efforts are "owned" by the program and business managers at the agencies who are accountable for the success of their entire program, including security. This essential aspect was underscored in GAO's Executive Guide. By working through the CIO Council and the President's Management Council, we will be able to improve coordination of security requirements and link security measures to business risks and agency mission. In this way security programs will support, not restrict, mission accomplishment.

The draft report also states that while federal information security has received increased visibility and attention since September 1996, central oversight remains limited and a comprehensive strategy has not been developed. The draft thus concludes that many aspects of the recommendations made in GAO's 1996 report, "Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110) remain applicable. We reiterate in part the response we made at that time, i.e., "The central thrust of the ITMRA is to increase the authority, responsibility, and accountability of Federal agencies for the management of their information resources. Ultimately we are concerned that the report's overemphasis on OMB's role could distract program managers in the Federal agencies from their primary responsibility for assuring information security."

On the draft report's recommendation to OMB and the NSC that the "various existing and newly initiated [via PDD-63] efforts to improve federal information security are coordinated under a comprehensive strategy," we are confident that the CIO Council's strategic plan as well as the plan of the Council's security committee along with the efforts we have described above address that recommendation.

Sincerely,

G. Edward DeSeve
Acting Deputy Director
for Management

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Jean H. Boltz, Assistant Director, (202) 512-5247
Ronald W. Beers, Assistant Director
Darrell L. Heim, Assistant Director
Carol A. Langelier, Assistant Director
Crawford L. Thompson, Assistant Director
Gregory C. Wilshusen, Assistant Director
Gary R. Austin, Senior Information Systems Analyst
Kirk J. Daubenspeck, Senior Information Systems Analyst
Ernest A. Döring, Senior Evaluator
Michael W. Gilmore, Senior Information Systems Analyst
William F. Wadsworth, Senior Information Systems Analyst

Atlanta Field Office

Sharon S. Kittrell, Senior EDP Auditor

Dallas Field Office

David W. Irvin, Assistant Director
Debra M. Conner, Senior EDP Auditor
Shannon Q. Cross, Senior Evaluator
William H. Thompson, Senior Evaluator
Charles M. Vrabel, Senior EDP Auditor

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