United States General Accounting Office

GAO

Report to Congressional Requesters

September 1996

INFORMATION SECURITY

Opportunities for Improved OMB Oversight of Agency Practices

GAO
75 years
1921 - 1996

GAO/AIMD-96-110

GAO

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

Accounting and Information
Management Division

B-272153

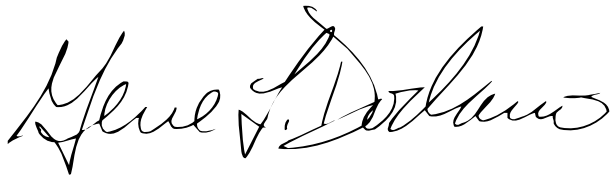
September 24, 1996

Congressional Requesters

Because of concern regarding the security of federal information systems and the data they maintain, Senator John Glenn, Ranking Minority Member, Senate Committee on Governmental Affairs, requested that we begin to examine information security issues on a governmentwide basis. Subsequently, Senator Ted Stevens, Committee Chairman, also expressed interest in these issues. As an initial step in response to these concerns, this report summarizes the results of recent audits of information security at major federal agencies. It also describes the Office of Management and Budget's oversight of federal agency practices regarding information security and details recommendations for improvement.

We are sending copies of this report to the Director of the Office of Management and Budget, the heads of the 15 federal agencies covered by our review, and other interested parties. Copies will be provided to others on request.

If you have any questions about this report, please call Christopher W. Hoenig, Director, Information Management Resources/Policies and Issues, on (202) 512-6208. Other major contributors to this report are listed in appendix II.



Gene L. Dodaro
Assistant Comptroller General

Executive Summary

Purpose

As federal agencies expand their reliance on automated and interconnected information systems, they face an increasing challenge to protect the integrity, confidentiality, and availability of the data they maintain. Although they have relied on computers for years, federal agencies, like businesses and other organizations throughout the world, are experiencing an explosion in the growth of electronic data and networked computer systems. The Department of Defense, alone, has a vast information infrastructure that includes 2.1 million computers, 10,000 local networks, and 100 long-distance networks. In addition, Defense uses the Internet, a global network interconnecting thousands of computer networks, to exchange electronic mail, log on to remote computer sites, and obtain files from remote locations. Civilian agencies are also increasingly reliant on automated, often interconnected, systems, including the Internet, to support their operations.

These advances promise to streamline federal operations and improve delivery of federal services. However, they also increase the potential risks that sensitive and critical information could be inappropriately modified, disclosed, or destroyed, possibly resulting in significant interruptions in service, monetary losses, and a loss of confidence in the government's ability to protect confidential data on individuals. The potential risks are increasing because automated systems and records are fast replacing manual procedures and paper documents, which in many cases are no longer available as "backup" if automated systems should fail. These vulnerabilities are exacerbated because, when systems are interconnected to form networks or are accessible through public telecommunication systems, they are much more vulnerable to anonymous intrusions from remote locations. Recent tests at the Department of Defense show that the number of attacks on Defense systems is growing dramatically and that many attacks are not detected.

Much of the information maintained by federal agencies, although unclassified, is extremely sensitive, and many automated operations would be attractive targets for individuals or organizations with malicious intentions, such as committing fraud for personal gain or sabotaging federal operations. Examples include law enforcement information maintained by the Federal Bureau of Investigation; import entry information maintained by the Customs Service; taxpayer data; commercial transactions; payroll, personnel, and health records; defense operational plans; electronic benefit payment records; and electronically submitted medicare claims.

Fully understanding the ramifications of information security weaknesses throughout the federal government has become an urgent issue. Without determining the extent of threats, vulnerabilities, and agency capabilities to manage their security programs, our government will remain ill-equipped to cope with significant new security problems and take advantage of opportunities for improved protection. This report summarizes the results of GAO's review of recent audits and self assessments at 15 major federal agencies to identify reported information security weaknesses. These 15 agencies accounted for over 98 percent of all federal outlays during fiscal year 1995. The report also describes the Office of Management and Budget's (OMB) oversight of federal agency practices regarding information security and identifies opportunities for improved oversight. The review was performed as an initial step in responding to requests from the former and current chairmen, Senate Committee on Governmental Affairs, that GAO examine a range of federal information security issues.

Background

The need to protect sensitive and critical federal data has been recognized for years in various laws, including the Privacy Act of 1974; the Paperwork Reduction Act of 1980, as amended; and the Computer Security Act of 1987. However, information security has taken on new significance as both reliance on computers and vulnerabilities associated with networked systems have increased. This is because the same techniques that agencies are employing to help cut costs and improve service—interconnected systems, readily accessible information, and paperless processing—are also factors that increase the vulnerability of operations and data to unauthorized modification and disclosure and to potentially devastating interruptions in service. Agency managers have the primary responsibility for ensuring the security of their information resources, and they are in the best position to assess the risks associated with their programs and to develop and implement policies to mitigate these risks. However, since enactment of the original Paperwork Reduction Act in 1980, OMB has been responsible for developing governmentwide guidance on information security and overseeing agency practices. Because of the breadth, significance, and complexity of this oversight challenge, it is important that OMB develop all possible strategies and assets—especially processes, staff expertise, and relevant information—to support its relatively small staff in fulfilling this responsibility.

Results in Brief

Audit reports and agency self assessments issued since September 1994 show that weak information security is a widespread problem that puts billions of dollars of federal assets at risk of theft, misuse, or loss, and threatens vast amounts of sensitive data, including personal data on individuals, with unauthorized disclosure. In addition to losses and inappropriate disclosures, weaknesses such as poor controls over access to data and inadequate disaster recovery plans diminish the reliability of the enormous amounts of electronically maintained information essential for delivering federal services, assessing the success of federal programs, and monitoring agency performance. An underlying cause is that agencies have not implemented information security programs that establish appropriate policies and controls and routinely monitor their effectiveness.

During the period in which these weaknesses were reported, OMB took steps to develop and improve federal guidance pertaining to information security. It also monitored, on an exception basis, agency efforts to address recognized major information security problems or potential problems affecting individual agency programs and systems. However, OMB's oversight efforts were uneven, and OMB generally did not proactively attempt to identify and promote resolution of fundamental security program weaknesses that are likely to be at the root of these problems. Identifying and correcting such weaknesses are essential elements in ensuring that agency policies and related management and technical controls are effectively implemented on a continuing basis.

OMB can improve its oversight effectiveness by taking advantage of the increasing amount of audit information on information security that is becoming routinely available as a by-product of agency financial statement audits required under the Chief Financial Officers (CFO) Act. Although these audits pertain primarily to financial systems, they are the only independent assessments of information security available at most major agencies on an annual basis. OMB can use this audit information, in conjunction with the results of agency self assessments, to evaluate the scope and adequacy of information security reviews at individual agencies and to monitor progress in correcting identified problems. Also, the recently established Chief Information Officers' (CIO) Council, which will be chaired by OMB, can serve as a mechanism for strategically addressing information security on a governmentwide basis. However, it is important that OMB develop better sources of information and staff expertise for proactively and systematically overseeing the overall design and effectiveness of agency information security programs.

Principal Findings

Information Security Weaknesses Are Widespread

Over the past 4 years, GAO has issued over 30 reports describing serious information security problems at major federal agencies, and agency inspectors general have issued numerous others. Our analysis of the most recent of these reports for the 15 largest federal agencies found that 10 agencies had serious information security weaknesses, some of which have existed for years. Material weaknesses were not reported for the other five agencies. However, independent reviews of computer-related controls at three of these five agencies were either not performed or were very limited.

The most common problems reported were (1) poor controls over access to sensitive and critical data and (2) incomplete and untested disaster recovery plans—weaknesses that essentially preclude an agency from reasonably ensuring the integrity, confidentiality, and availability of critical and sensitive computerized data, such as taxpayer information and federal financial records. Examples include the following:

- Estimates by the Department of Defense indicate that attacks on unclassified computer systems and networks are a serious and growing threat to our national security, including Defense's ability to execute military operations and protect sensitive information. Defense data indicate that Defense may have experienced as many as 250,000 attacks in 1995 and that the number of attacks is doubling each year. Successful attacks by outside intruders have shut down systems and corrupted sensitive data. However, estimates based on tests conducted since 1992 showed that less than 1 percent of attacks on Defense's systems were detected and reported. Although no summary costs have been developed, Defense officials estimate that the cost of such incidents is at least tens of millions of dollars per year.
- Annual audits since 1993 have found that due to poor computer controls, IRS cannot ensure that the confidentiality and accuracy of taxpayer data are protected and that the data are not manipulated for purposes of individual gain. Specifically, (1) controls have not prevented users from unauthorized access to sensitive programs and data files, (2) numerous users have been allowed powerful access privileges that could allow circumvention of existing controls, and (3) security reports used to monitor and identify unauthorized access to the system are cumbersome and virtually useless to managers for monitoring activity.

- In March 1995, the Office of Personnel Management Inspector General reported that federal retirement program assets were "highly vulnerable to loss or misuse" because of electronic data processing weaknesses, primarily excessively broad user access privileges, related to systems that maintained 2.1 million annuitant files and generated $36 billion in benefit payments during fiscal year 1994.

Individual audit reports describe varying causes for specific weaknesses at individual agencies. However, our audits have shown that an underlying factor is poorly managed security programs that do not proactively and systematically assess risk, monitor the effectiveness of security controls, and respond to identified problems. Such programs are essential to ensure that management and technical controls, including actions to correct identified weaknesses, are effective on a continuing basis.

Central Policy Has Been Updated

As part of its various efforts to explore and develop policies associated with a range of information security issues, in February 1996, OMB issued a revised version of its central guidance to agencies on developing an effective information security program. Like the previous version, issued in 1985, the revised Circular A-130, Appendix III, "Security of Federal Automated Information Resources," establishes a minimum set of management controls that are to be included in federal automated information security programs. These include assigning responsibility for security, developing a system security plan, screening and training individual users, assessing risk, planning for disasters and contingencies, and reviewing security safeguards at least every 3 years. However, unlike the previous version, the revised appendix recognizes that all federal computer systems require some level of protection, not just systems judged to be "sensitive." 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. OMB worked extensively with the National Institute of Standards and Technology, agency security managers, and others to develop the revised Appendix III. Written comments submitted by numerous organizations and individuals and the remarks of agency officials that GAO interviewed indicate that the revised guidance is generally considered to be a valuable and necessary update that recognizes the increasingly open and interconnected computer systems that support agency operations.

Monitoring of Agency Practices Has Been Uneven

Comprehensive oversight requires independently identifying management issues, focusing attention on these issues, and ensuring appropriate resolution of identified problems. Policy analysts in OMB's Office of Information and Regulatory Affairs and program examiners in OMB's Resource Management Offices have monitored selected security issues at individual agencies. However, the scope and depth of efforts intended to uncover critical information security issues vary among agencies, and these efforts are often reactive. GAO met with OMB program examiners for 11 agencies. Of these, examiners for eight agencies essentially reacted to recognized problems, saying that they had little expertise regarding information resource management and related security issues. They said that they only considered security when it was raised as a significant issue by agency managers or auditors and, then, usually as it pertained to a specific program or system. Examiners for two other agencies had taken a somewhat more proactive look at the agencies' automated operations, including security; while the examiner for the remaining agency said that program examiners almost never considered systems-related issues, including security, as part of their examinations.

As for focusing on management issues, although OMB's revision of Circular A-130 focused general attention on the importance of information security programs, OMB has not systematically monitored compliance with its guidance or the effectiveness of security programs at individual agencies, even though problems in several agencies have been reported for years. While analysts in OMB's Office of Information and Regulatory Affairs have gained a high-level understanding of agency programs through informal discussions with agency personnel, most program examiners, who usually obtain more detailed information about individual agency operations, generally do not consider the effectiveness of an agency's overall information security program.

Information for Oversight Is Limited

OMB obtains little documented information to help it proactively oversee agency information security programs. It has routinely obtained agency annual internal control assessments required under the Federal Managers Financial Integrity Act and Strategic Information Resource Management Plans. However, these documents vary significantly in level of detail regarding security issues and are often of little value for overseeing security practices. OMB generally does not obtain the more detailed self assessments of information security that agencies should be using as the basis for these summaries.

OMB program examiners cited independent audit reports as one of their most useful sources of information because they provided an independent assessment of agency operations. However, in the past, independent audits of computer security have not routinely been performed for all major agencies. Audits performed under the CFO Act of 1990 promise to make such independent audit information more routinely available because, in practice, such audits generally include evaluating and testing controls over information security. In the early 1990s, selected segments of federal operations became subject to annual financial statement audits under the Act, and in 1994, this audit requirement was extended to all major federal entities by the Government Management Reform Act. As a result, the percentage of federal expenditures that is audited has been steadily growing, and is expected to reach 98 percent by fiscal year 1997.

However, significant aspects of some agencies' operations, such as those involving sensitive medical records, are not likely to be covered by financial statement audits. For this reason, it is important for OMB, as well as agency managers, to coordinate their reviews of CFO Act audit reports and their reviews of other types of information security assessments, such as self assessments. When viewed together, these audits and assessments may provide a more comprehensive view of agency information security and allow OMB and agency officials to identify gaps in review coverage.

CIO Council and Financial Audit Reports Offer Opportunities for Improved Oversight

In light of the growing significance of information security and the widespread reported weaknesses, it is essential that OMB take advantage of all opportunities to leverage its resources and take advantage of available information. In this regard, OMB can analyze the increasing amount of audit information that is becoming available due to recently expanded requirements for annual financial statement audits of federal agencies, under the CFO Act. Although CFO Act audits pertain primarily to financial management systems, OMB's Office of Information and Regulatory Affairs and Office of Federal Financial Management could use them, in conjunction with agency self assessments, to determine if all key systems had been reviewed at an individual agency and to monitor actions to correct reported information security problems.

Also, the recently established CIO Council can serve as a forum for addressing governmentwide information security issues, raising security awareness, and developing a strategic approach to better understanding the security problems facing federal agencies and improving federal information security programs. The Council, established in July 1996

through Executive Order, is intended to be "the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources." It is chaired by OMB's Deputy Director for Management, and its membership includes CIOs at all major federal agencies.

Recommendations

To enhance OMB's ability to oversee and improve federal information security programs, GAO is making the following recommendations to the Director of OMB:

- Advocate and promote the CIO Council's adoption of information security as one of its top priorities and development of a strategic plan for (1) increasing awareness of the importance of information security, especially among senior agency executives, and (2) improving information security program management governmentwide. Initiatives that the CIO Council should consider incorporating in its strategic plan include
  - 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 using interagency teams of reviewers;
  - 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.
- Direct the Office of Information and Regulatory Affairs, the Office of Federal Financial Management, and the Resource Management Offices to (1) supplement their current reviews of audit reports to include reviewing audits conducted under the CFO Act in order to identify any findings related to information security and (2) use this information, in conjunction with reports on agency self assessments, to assist in proactively monitoring the scope of such reviews and the effectiveness of agency information security practices.
- Encourage the development of improved sources of information with which to monitor compliance with OMB's guidance and the effectiveness of

agency information security programs. This could include engaging assistance from private contractors or others with appropriate expertise, such as federally funded research and development centers.

- Direct the Office of Information and Regulatory Affairs to develop and implement a program for increasing 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.

Agency Comments and Our Evaluation

In written comments on a draft of this report, OMB agreed that information security is an important management issue and stated that certain of the report's recommendations are meritorious. In particular, OMB said that it will encourage the CIO Council to adopt information security as one of its top priorities and that it will review (1) the training and related materials provided to program examiners and (2) the availability of improved sources of information. However, OMB disagreed with the report's tone, which it characterized as suggesting "that OMB has not been dedicating sufficient resources in the past to overseeing the agencies' information security activities, and that therefore OMB in the future should dedicate more of its resources to this objective." In addition, OMB stated its concern that the report overemphasizes OMB's role and that this could distract federal agencies from their responsibilities as the primary managers of federal information security.

GAO agrees that agency managers are primarily responsible for information security. GAO's audit efforts related to information security over the past few years have focused almost exclusively on individual agency practices, and it has made dozens of related recommendations to agency officials. Thirty products resulting from this work and containing these recommendations are listed at the end of this report. The results of this work led GAO to identify a pattern of governmentwide information security weaknesses.

In light of the pattern of weaknesses that GAO has identified and the increasing importance of information security in virtually every aspect of federal operations, OMB has a vital leadership role to play in promoting and overseeing agency security practices. This role was recently reemphasized in the Information Technology Management Reform Act of 1996 and in revisions to the Paperwork Reduction Act, which together explicitly outline OMB's responsibilities for overseeing agency practices regarding information privacy and security. Information security has become a

consideration in the management of virtually every major federal program and in billions of dollars in annual information technology investment decisions. For these reasons, GAO believes that information security, as well as other information management issues, merits a high priority relative to other budget and management issues.

In this regard, GAO's recommendations are focused primarily not on increasing the amount of OMB resources but on increasing the impact of OMB's current resources by taking advantage of newly available audit information, discussed in chapter 4, and by expanding staff expertise. These actions, at a minimum, are needed to help address growing concerns over the adequacy of federal information security. GAO also believes that periodic oversight reviews of agency information security programs would be beneficial but that such reviews could be performed by interagency teams under the auspices of the OMB-chaired CIO Council, as suggested in chapter 4.

Contents

Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
FFELP	Federal Family Education Loan Program
FMFIA	Federal Managers' Financial Integrity Act
HHS	Department of Health and Human Services
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
RMO	Resource Management Office
VA	Department of Veterans Affairs

Introduction

As federal agencies expand their use of information technology, they face an increasing challenge to protect the integrity, confidentiality, and availability of information that is vital to their missions. Like the nation as a whole, our government is becoming increasingly dependent on widely interconnected computer systems and the electronic data they maintain. These systems and data are essential to carry out critical operations, such as tax collections; safeguard billions of dollars in assets, such as military equipment and accounts receivable; and deliver basic services, such as social security payments and other benefits. Reliance on these systems and on electronic data is revolutionizing the way that agencies collect, process, store, and disseminate information. However, without effective controls, such reliance also can increase the risks of financial loss, unauthorized access to sensitive information, and devastating interruptions in service.

To provide a governmentwide overview, this report summarizes the results of our reviews of information security at individual agencies and of similar assessments performed by others. The report also describes OMB's oversight of federal agency practices regarding information security and identifies opportunities for improvement. We performed this review in response to a request from Senator John Glenn, Ranking Minority Member, Senate Committee on Governmental Affairs, that we examine a broad range of federal information security issues. Subsequently, Senator Ted Stevens, Committee Chairman, also expressed interest in these issues.

Increased Reliance and New Vulnerabilities Combine to Underscore Importance of Adequate Information Security

Information security is a growing concern because the federal government, like the nation as a whole, is becoming increasingly dependent on computerized information systems and electronic records. These systems and records are fast replacing manual procedures and paper documents, which in many cases are no longer available as "backup" if automated systems should fail. The potential risks associated with reliance on electronic systems and records are exacerbated because more and more systems are being interconnected to form networks or are accessible through public telecommunication systems, making the systems themselves and the data they maintain much more difficult to protect from unauthorized users or outside intruders.

All major agencies rely on computer systems to provide critical support for their operations, and even greater reliance is planned for the future. In addition, agencies are increasing their use of interconnected systems and

electronically transmitted data in order to streamline operations, make federally maintained data more accessible, and reduce paperwork.

Most notably, the Department of Defense has a vast information infrastructure that includes 2.1 million computers, 10,000 local networks, and 100 long-distance networks. The majority of the information maintained on Defense's computers is sensitive but nonclassified data essential to daily operations, such as commercial transactions; payroll, personnel, and health records; operational plans; and weapons systems maintenance records. In addition, Defense uses the Internet, a global network interconnecting thousands of computer networks, to exchange electronic mail, log on to remote computer sites, and obtain files from remote locations.

Civilian agencies are also increasingly reliant on interconnected systems, including the Internet, and on electronic data. The following examples illustrate just a few of the ways that agencies are expanding their use of information technology to support critical operations.

- Law enforcement officials throughout the United States and Canada rely on the Federal Bureau of Investigation's National Crime Information Center computerized database for access to sensitive criminal justice records on individual offenders. According to the Bureau's fiscal year 1997 budget submission, the system is available to 78,000 authorized users and processes an average of about 2 million transactions daily.
- The Internal Revenue Service (IRS), which relies on computers to process and store millions of taxpayer records, views electronic filing of tax returns as fundamental to its future operations. The number of individual income tax returns filed electronically increased from 4.2 million in 1990 to about 14.8 million for the first 3 and a half months of 1996. IRS goals include significantly increasing the number of electronically filed returns and eventually eliminating paper returns for a large segment of filers.
- The Customs Service relies on automated systems to process entry declarations, which totaled over 39 million in fiscal year 1994 and led to payment of over $20 billion in duties. Although many entry declarations are submitted as paper documents, a growing number are submitted electronically.
- The Department of Agriculture is reducing the use of paper food stamp coupons through its electronic benefits transfer program. Under the program, individual recipients' monthly benefits are recorded in a central computer file. Individuals then use "credit card" type cards with secret personal identification numbers to draw on these benefits and pay for

their groceries. During fiscal year 1995, about 630,000 households participated in the electronic benefit transfer food stamp program. According to the Federal Electronic Benefits Transfer Task Force, the program could potentially cover over 10 million households.

- Medicare part B claims that were submitted and processed electronically jumped from 36 to 72 percent between 1990 and 1994, and further increases are likely. Medicare part B covers physician services, outpatient hospital care, medical supplies, and other health benefits, such as emergency ambulance service. The program cost $60 billion in fiscal year 1994, and, according to OMB, costs are expected to double over the subsequent 7 years.

Unfortunately, the same factors that are so important to streamlining federal operations—interconnected, often widely-dispersed systems; readily accessible information; and paperless processing—are also factors which increase the vulnerability of these operations and data. Specifically, the threats to agency systems and the potential for harm have increased because

- the move to more interconnected systems has provided greater numbers of individuals access to extensive databases of information through widely distributed networks of computers;
- agencies are placing greater reliance on electronic records, in some cases eliminating paper records; and
- intruders, including criminals, are becoming more skilled at defeating security techniques designed to protect computer systems and electronic information.

When systems are not adequately protected the potential for malicious and criminal acts is enormous. For example, by obtaining access to data files, an individual could make unauthorized changes for personal gain, such as diverting payments or reducing amounts owed on debts. Similarly, an individual could obtain sensitive information about business transactions or individuals, which could then be sold or used for malicious purposes. By obtaining access to computer programs, an individual could make unauthorized changes to these programs, which in turn could be used to access data files or to process unauthorized transactions, such as improper payments. Also, an intruder could eliminate evidence of unauthorized activity, thus, significantly reducing the likelihood that such activity would ever be detected.

Further, in an inadequately protected network environment, an agency's operations could be sabotaged from remote locations by altering or destroying critical data and programs, or by introducing malicious code, such as viruses, to damage or congest system operations. Significant damage could also occur as a result of accidental errors and deletions by authorized users. Regardless of the individual user's intent, in today's high-speed, highly automated, and interconnected computing environment, thousands of transactions could be erroneously processed or enormous amounts of data could be destroyed or disclosed before an agency detected the damage.

In addition to access control risks, computer facilities and electronic media can be damaged or otherwise rendered unusable by fires, floods, contamination, and other manmade and natural disasters. If an agency does not have adequate contingency plans and preparations for such unexpected events, it may be forced to suspend critical operations or it could lose data and software that are difficult and costly, or even impossible, to replace.

Responsibilities Outlined in Laws and OMB 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."

The adequacy of controls over computerized data is also addressed indirectly by the Federal Managers Financial Integrity Act (FMFIA) of 1982 (31 U.S.C. 3512(b) and (c)) and the Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576). FMFIA 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 CFO Act requires agency CFOs to develop and maintain financial management systems that provide

complete, reliable, consistent, and timely information. Under the act, major federal agencies annually issue audited financial statements. In practice, such audits generally include evaluating and testing controls over information security.

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 review system security at least every 3 years. 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. OMB, NIST, and agency responsibilities regarding information security were recently reemphasized in the Information Technology Management Reform Act of 1996.

Objectives, Scope, and Methodology

Our objectives were to (1) provide a general overview of the adequacy of federal information security at major federal agencies based on reported information, (2) identify and categorize the most significant information security weaknesses reported, (3) identify the general causes of reported weaknesses, and (4) assess OMB's efforts to oversee agency information security practices. To accomplish these objectives we analyzed the results of our evaluations of computer-related controls at five major agencies since June 1993. These agencies included the Internal Revenue Service and the U.S. Customs Service, which are both part of the Department of the Treasury; the Department of Education; the Department of the Army; and the Department of Housing and Urban Development. We performed most of these assessments as part of our financial statement audits at these agencies. While such audits focus on the security of the data supporting the financial statements, they include evaluations and tests of general controls that affect a significant segment of the agencies' computerized operations. A list of GAO reports and testimonies that address the adequacy of information security at federal agencies is provided at the end of this report.

We supplemented reviews of our own audits with an analysis of 149 other reports on major federal agencies to determine if information security weaknesses had been reported and, if so, what types of weaknesses were reported. The reports we reviewed resulted from independent audits by agency inspectors general issued between September 1992 through March 1996, and from agency self assessments required under FMFIA for fiscal years 1994 and 1995. The agencies covered included the Departments of Agriculture, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Justice, Labor, Transportation, the Treasury, and Veterans Affairs; the General Services Administration; the National Aeronautics and Space Administration; the Social Security Administration; and the Office of Personnel Management. Together, our analyses covered the 15 major departments and agencies that are responsible for spending or safeguarding the largest amounts of federal resources. In total, these agencies accounted for over 98 percent of all federal outlays during fiscal year 1995.

We based our analyses almost exclusively on reported findings. Although we spoke with inspector general audit managers at several agencies to clarify information that had been reported, we did not assess the quality or completeness of any of the inspector general audits or agency self assessments covered by our survey.

To augment information included in reports on individual agencies, we met with members of the steering committee of the Federal Computer Security Managers Forum, an information-sharing group established by NIST, and we reviewed various OMB and NIST documents, as well as related laws.

To obtain information on OMB's oversight efforts, we met with officials from OMB's Office of Information and Regulatory Affairs (OIRA), Office of Federal Financial Management, and Resource Management Office branches responsible for overseeing programs at 11 of the 15 agencies included in our review. In addition, we met with senior information resource management officials and security program managers at five agencies to discuss their interactions with OMB and other agencies responsible for providing guidance and assistance regarding information security issues. These five agencies are the Departments of Agriculture, Health and Human Services, Treasury, and Transportation and the Office of Personnel Management.

Our review was performed in Washington, D.C., from July 1995 through May 1996 in accordance with generally accepted government auditing standards. We requested written comments on a draft of this report from the Acting Director of OMB or his designee. OMB's Deputy Director for Management provided written comments on a draft of this report. These comments are discussed in the "Agency Comments and Our Evaluation" section of chapter 5 and are reprinted in appendix I.

Audits and Self Assessments Have Identified Serious Weaknesses That Increase Risks

Recent audits show that weak information security is a serious governmentwide problem that is putting major federal operations at risk. Between September 1994 and April 30, 1996, serious weaknesses were reported for two-thirds of the agencies covered by our review, and for half of these agencies the weaknesses had been reported for at least 5 years. A fundamental cause of these weaknesses is that agencies have not implemented security programs that provide a systematic means of assessing risk, implementing effective policies and control techniques, and monitoring the effectiveness of these policies and techniques.

Significant Weaknesses Have Been Reported for Most Major Federal Agencies

Of the 15 agencies included in our review, serious information security control weaknesses were reported for 10 from September 1994 through April 1996. The two most commonly reported weakness indicate fundamental deficiencies in the ability of agencies to protect federal information and the continuity of federal operations. The first was poor access control, which increases the risk that an individual or group could inappropriately modify or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. The second most commonly reported weakness was inadequate disaster planning, which increases the risk that an agency will not be able to satisfactorily recover from an unexpected interruption in critical operations. Many of the identified weaknesses have remained uncorrected for years. Of the 10 agencies with reported weaknesses, FMFIA reports for 5 showed that the problems had remained uncorrected for 5 years or longer.

Examples of reported problems include the following:

- Estimates by the Department of Defense indicate that attacks on unclassified computer systems and networks are a serious and growing threat to our national security, including Defense's ability to execute military operations and protect sensitive information. Defense data indicate that Defense may have experienced as many as 250,000 attacks in 1995 and that the number of attacks is doubling each year. Successful attacks by outside intruders have shut down systems and corrupted sensitive data. However, estimates based on tests conducted since 1992 showed that less than 1 percent of attacks on Defense's systems were detected and reported. Although no summary costs have been developed, Defense officials estimate that the cost of such incidents is at least tens of millions of dollars per year.[1]

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

- During our audit of the IRS' fiscal year 1995 financial statements, we found that, as reported since 1993, controls over sensitive information were inadequate.[2] Although corrective actions are under way, as detailed in previous reports, IRS could not ensure that the confidentiality and accuracy of taxpayer data were protected and that the data were not manipulated for purposes of individual gain. Specifically, (1) controls did not prevent users from unauthorized access to sensitive programs and data files, (2) numerous users were allowed powerful access privileges that could allow circumvention of existing controls, and (3) security reports used to monitor and identify unauthorized access to the system were cumbersome and virtually useless to managers for monitoring activity. In addition, back-up and recovery plans were inadequate to provide reasonable assurance that IRS service centers could recover from disasters.[3]
- In June 1994, we reported a variety of computer-related control weaknesses at the Customs Service, including that thousands of internal and external users had inappropriate access to critical and sensitive programs and data files.[4] In May 1995, the Department of the Treasury Inspector General reported that despite attempts to correct the problem, the weaknesses continued to exist.[5]
- In June 1994 and June 1995, we reported that controls over the Department of Education's Federal Family Education Loan Program (FFELP) did not adequately protect sensitive data files, application programs, and systems software from unauthorized access, change, or disclosure. These controls are critical to Education's ability to safeguard FFELP assets, maintain sensitive loan data, and ensure the reliability of financial management information about the program. The Department reported that FFELP had $77 billion in outstanding loan guarantees as of September 30, 1994.
- The Department of Health and Human Services (HHS) first reported the lack of a formal, well-coordinated system security program in its Administration for Children and Families in its fiscal year 1990 FMFIA report. In December 1995, HHS reported that the Administration still had not implemented fundamental computer security program elements such

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

[3]Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/AIMD-95-141, August 4, 1995) and IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, September 22, 1993).

[4]Financial Audit: Examination of Customs' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-119, June 15, 1994).

[5]Audit of the United States Customs Services Fiscal Year 1994 Financial Statements, OIG-95-071, May 1, 1995.

as risk assessments and independent reviews of contingency plans for sensitive systems supporting this $17 billion dollar per year program.

- The Department of Justice first recognized automated data processing security as a weakness in 1985. Although Justice reported in February 1996 that it has made departmentwide security improvements, it also reported that some components had not completed and tested continuity of operations plans, developed policies for computer and telecommunications security, or conducted required risk assessments of component computer systems.
- In March 1995, the Department of Agriculture's Inspector General reported that controls over access to computer software programs and data were inadequate to prevent unauthorized activity at the Department's National Finance Center.[6] The Center processes billions of dollars in payments and sensitive information for itself and other agencies, including payroll, retirement savings, administrative and travel payments, and property management information.
- In March 1995, the Office of Personnel Management Inspector General reported that federal retirement program assets were "highly vulnerable to loss or misuse" because of electronic data processing weaknesses, primarily excessively broad user access privileges, related to systems that maintained 2.1 million annuitant files and generated $36 billion in benefit payments during fiscal year 1994.

Serious information security weaknesses may also exist for some of the five agencies for which no weaknesses were reported. This is because audit reports at one agency specifically stated that computer-related controls had not been reviewed as part of the audit. Also, audit managers at two other agencies said that their computer audit capabilities were limited, and they could not readily determine what, if any, work they or their contractors had performed in this area.

For the 10 agencies with serious reported weaknesses, auditors made 90 new recommendations for specific corrective actions in reports issued from September 1994 through May 1996. In addition, these reports referred to numerous recommendations made in prior years that had not yet been fully or effectively implemented.

Although most agencies have reported actions initiated or planned to correct their weaknesses, a recurring condition reported in GAO, inspector general, and FMFIA reports is that agency actions, while resulting in some

[6]U.S. Department of Agriculture Fiscal Year 1994 National Finance Center General Controls Review, New Orleans, Louisiana (OIG, Audit Report No. 11600-3-FM, March 1995).

improvement, are not completed promptly and do not adequately address identified problems. Recent audits at IRS, Education, and Customs all found that, while some improvements had been made, corrective actions at those agencies had been repeatedly delayed or were incomplete.

As with Defense, the costs of agencies' information security weaknesses cannot be determined because agencies generally do not keep summary records of security violations or account for the cost of responding to such violations. In addition, due to poor controls and lack of user awareness, it is possible that many violations are not being detected or reported.

Poor Security Program Management Is an Underlying Cause

A well designed and managed security program with senior-level support is essential for ensuring that an agency's controls are appropriate and effective on a continuing basis. In this regard, managing information security is similar to managing risks associated with other aspects of agency operations. The program should establish a process and assign responsibilities for systematically (1) assessing risk, (2) promoting user awareness of security issues, (3) developing and implementing effective security policies and related control techniques, (4) monitoring the appropriateness and effectiveness of these policies and techniques, and (5) providing feedback to managers who may then make adjustments as needed. Such a program can provide senior officials a means of managing information security risks and the related costs rather than just reacting to individual incidents.

Without a well designed and managed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be ineffective or inconsistently applied. Such conditions generally result in insufficient protection of sensitive or critical resources and, conversely, may result in disproportionately high expenditures for controls over low-risk resources.

Individual audit reports describe varying causes for specific control weaknesses at individual agencies. However, in our reviews of information security controls, we found that the major underlying factor was lack of a well managed information security program with senior management support. For example, in May 1996, we reported that Defense had not established a comprehensive computer security program and had not assigned responsibility for ensuring that such a program was implemented. As a result, Defense information security policies were dated, inconsistent, and incomplete; user awareness was insufficient; and security personnel

were inadequately trained. Similarly, in August 1995, we reported that IRS had no proactive, independent information security group that was systematically deployed to review the adequacy and consistency of security over IRS' computer operations. Instead, IRS was addressing information security issues on a reactive basis. In June 1995, we reported that information security weaknesses at Education resulted from the Department's overall weak security administration and failure to develop and implement key policies and procedures. Several of the inspector general audit reports that we reviewed also indicated that agency managers were not taking the steps needed to ensure that controls had been implemented and were operating properly.

To gain an additional perspective on the causes of poor controls, we met with selected members of the steering committee of the Federal Computer Security Managers Forum, an information-sharing group established by NIST. These officials said that additional support from senior management would allow them to establish more effective programs. According to forum members, a lack of management support can result in inadequate resources devoted to information security, a situation that limits the ability of security program managers to address security needs proactively.

A number of factors can contribute to the perception of a lack of senior management support for information security. First, as with other types of internal controls, senior managers may view security efforts as impediments to the efficient accomplishment of the agency's mission. This is because security controls cost money to implement and monitor, and, generally, they diminish the ease with which systems and data can be accessed and updated. In addition, some senior managers may be unaware of the full range of threats and vulnerabilities that must be considered when determining what level of information security is adequate. Others may not have the data they need to make informed decisions. As a result, they may want to adopt information technology for new applications without adequately considering the related risks, or they may be unwilling to strengthen security over existing procedures. A comprehensive security program can help senior managers maintain an appropriate balance between operational efficiency and security by systematically and continually fine-tuning policies and control procedures through a risk assessment, monitoring, and feedback cycle.

As agency systems become more interconnected and open to large numbers of outside users and as more sophisticated technical controls become available, the effort needed to manage agency systems and

monitor the effectiveness of related controls will become more complex and more time-consuming. The benefits of better service and lower processing costs should far outweigh the cost of these additional security efforts. However, it will be important for senior managers to recognize the security challenges involved and to help their organizations successfully meet these challenges.

Guidance to Agencies Has Been Updated, but Oversight Has Been Uneven

OMB has participated in a variety of efforts to develop governmentwide policies regarding federal information security, and it recently issued an updated version of its central guidance to agencies on minimum automated information security program requirements. OMB has also monitored agency efforts to address recognized security weaknesses or potential weaknesses related to individual agency programs or systems. However, OMB has not proactively attempted to identify and address the underlying causes of these problems, which often are rooted in the design and management of an agency's overall information security program. In addition, the depth and scope of OMB's monitoring efforts have varied significantly from one agency to another.

Although security program management is primarily the responsibility of agency managers, under the Paperwork Reduction Act, OMB is charged with overseeing the use of federal information resources, including providing direction and overseeing the "privacy, confidentiality, security, disclosure, and sharing of information." OMB oversees and guides agency operations through its three statutory offices, which are primarily responsible for setting policy, and its five Resource Management Offices (RMO),[1] which are primarily responsible for examining agency budget issues and overseeing agencies implementation of governmentwide management policies. The Office of Information and Regulatory Affairs (OIRA) is the statutory office responsible for establishing governmentwide information resource management policies, including those related to information security, and assisting the RMOs in overseeing agency implementation of these policies.

OIRA Has Focused on Developing and Communicating Policy Guidance

OIRA's information security oversight efforts are conducted primarily by its Information Policy and Technology Branch, which employs 10 individuals who regularly deal with governmentwide information resource management issues. Three of these individuals have routinely spent a significant amount of their time on information security issues.

Over the last few years the Branch has participated in various projects to address cross-cutting information security issues as part of its overall responsibility to establish information resource management policies.

[1]In 1994, OMB implemented a reorganization plan that replaced its former five budget program areas with five RMOs, redistributed staff, and created RMO program examiner positions to replace budget examiner positions. The intent of this reorganization, referred to as OMB 2000, was to integrate OMB's budget analysis, management review, and policy development roles and, thus, improve the decision-making process and oversight of executive branch operations. A detailed description of these changes is presented in our report entitled Office of Management and Budget: Changes Resulting From the OMB 2000 Reorganization (GAO/GGD/AIMD-96-50, December 29, 1995).

These include efforts to (1) develop federal policies on the use of cryptography, (2) define the federal role regarding the security of the national information infrastructure, (3) assist the General Services Administration in developing telecommunications security requirements, and (4) explore security issues related to electronic commerce. However, the Branch's most basic and comprehensive accomplishment regarding federal agency security practices was developing an updated version of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources."

Issued in February 1996, the revised Appendix III is intended to clarify guidance to agencies on managing information security as they increasingly rely on open and interconnected systems. Like the previous version, issued in 1985, the new appendix establishes a minimum set of controls that are to be included in federal automated information security programs. These include assigning responsibility for security, developing a system security plan, screening and training individual users, assessing risk, planning for disasters and contingencies, and reviewing security safeguards at least every 3 years. However, unlike the previous version, the revised appendix recognizes that all federal computer systems require some level of protection, not just systems judged to be "sensitive" by agency managers. 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. In developing the revised appendix, OIRA obtained significant input from agency managers, NIST, and the Computer System Security and Privacy Advisory Board,[2] including written comments from over 27 organizations and individuals, before issuing the final version.

Comments on the exposure draft of the revised Appendix III indicate that it is generally considered to be a valuable and necessary update to this central federal policy document that recognizes the increasingly open and interconnected computer systems that support agency operations. The senior information resource managers and security program managers that we met also generally agreed that OIRA had done a good job of developing and communicating guidance regarding information security and responding to their individual requests for clarification of guidance.

[2]The Computer System Security and Privacy Advisory Board was established by the Computer Security Act to identify emerging issues related to computer system security and privacy; to advise NIST on these issues; and to report its findings to OMB, the National Security Agency, the Secretary of Commerce, and appropriate committees of the Congress. It is composed of both federal and private sector representatives.

To assist in overseeing agency practices regarding information resource management, including security, analysts in OIRA's Information Policy and Technology Branch communicate frequently with RMO program examiners to (1) help ensure that the examiners are aware of high-risk or problem areas that affect the agency programs and (2) provide technical assistance to the RMOs, sometimes at the request of individual examiners. The Branch also attempts to maintain an understanding of agency practices through informal discussions with agency personnel and participation in various conferences and meetings. For example, the Branch's primary information security policy analyst estimates that he has made six to eight presentations at individual agencies per year and numerous presentations at professional conferences and meetings, such as those of the Computer System Security and Privacy Advisory Board. He has also routinely participated in the Federal Computer Security Managers Forum, which is sponsored by NIST and meets approximately every 4 to 6 weeks. At Forum meetings, he has the opportunity to talk directly with the individuals who are responsible for administering agency security programs.

However, OIRA does not systematically monitor agency compliance with OMB information security guidance or assess the effectiveness of agency information security management practices that are fundamental elements in the agencies' ability to effectively deal with information security risks and identified weaknesses. The most recent effort to methodically gain a relatively detailed overview of agency practices was completed in 1992. That effort involved a series of visits at each of 28 agencies by a team of OMB, NIST, and National Security Agency representatives. According to a January 1992 letter to the Director of OMB from the Computer System Security and Privacy Advisory Board, the visits were enthusiastically received and resulted in greater awareness on the part of senior officials, which, in turn, resulted in increased management support for agency computer security programs. In addition, the visits resulted in proposals for improving federal information security, most of which were incorporated in OMB's February 1996 revision of Circular A-130, Appendix III.

Despite the apparent success of the 1992 visits, Information Policy and Technology Branch officials said that they have no plans to repeat the effort because it was very resource intensive. They said that as a result, no systematic visits to agencies were currently planned and that any future efforts along this line would address a range of information resource management concerns in addition to security.

Engaging the services of contractors on a limited basis would be one means by which OMB could supplement its staff resources and periodically take a closer look at individual agency practices. Information Policy and Technology Branch officials told us that OMB has not customarily used contractors to assist in carrying out its oversight responsibilities. At GAO, we have found that engaging contractors to assist on individual projects can be a cost-effective means of expanding our ability to review agency operations, especially in areas such as information security where very specific and often highly technical expertise may be needed.

RMO Oversight of Information Security Practices Has Been Uneven

We met with branch chiefs and program examiners responsible for examining programs at 11 of the 15 agencies covered by our review and found that their attention to information security varied. Examiners for all but one agency said that they considered information security during their examination of agency budgets and programs to some extent, although examiners for eight agencies said that they only did so when it had been highlighted by agency management or in audit reports as a problem. These considerations were generally limited to monitoring agency progress in correcting recognized problems and did not involve examining an agency's information security program or the effectiveness of agency security practices in general. For example, the RMO branches overseeing the Departments of Agriculture and Education and the Office of Personnel Management all said that they had paid special attention to security issues associated with certain systems or facilities because weaknesses had been recently reported.

The program examiners and their branch chiefs said that information security is usually not closely examined because it is only one of many issues demanding their attention. The number of program examiners responsible for each agency varied from about 5 for the Department of Education to about 30 for the Department of Defense.[3]

There were a few cases where known problems were receiving virtually no attention from the RMOs. Most notably, the representative that we spoke with about the branches that oversee the Department of Defense said that the program examiners there almost never considered problems related to information systems, including security, because such issues did not seem to have a significant budget impact compared to other issues and

[3]These numbers are approximate, because program examiners are organized by programmatic issues, rather than strictly by agency. Most of the RMO branches we visited were responsible for one major department and one or more smaller agencies with related programs. However, in some cases, an agency's programs were divided among two or more branches.

programs. He emphasized that due to the Department of Defense's size and variety of programs, the Defense examiners had to be very selective in deciding which items merited examination. Also, a long-standing problem regarding a lack of disaster recovery planning at the Department of Veterans Affairs (VA) appeared to have prompted little interest from the RMO branch responsible for overseeing the Department, although other security issues were considered.

Officials in several branches indicated that they were becoming increasingly sensitized to the significance of information security due to recent operational issues within their agencies. For example, the VA Branch Chief said that VA's efforts to streamline its processes by accessing needed information in other agencies' systems had raised a number of concerns about the security of shared data and the related legal requirements. Similar concerns were expressed by the branches overseeing system modernization projects at the Department of Agriculture and the Health Care Financing Administration because these projects would result in increased accessibility of sensitive information on individuals.

Despite the increasing importance of information security, few of the program examiners said that they had any significant experience or expertise in dealing with information systems or related security issues. Most said that due to their lack of expertise, they depended largely on OIRA to help them understand the issues and assess related agency actions. Most of the branches said they had good working relationships with OIRA, as well as the other statutory offices within OMB, and that when they needed technical assistance, it was available. Also, some branches had informally designated an individual with some experience in examining systems-related issues to review these issues and to serve as a resource for other examiners in the branch. Two of the branches we visited each had a relatively experienced individual to assist in the branch's examinations. These individuals were very familiar with their agencies' information processing operations and appeared to have performed a much more comprehensive review of information security than had been performed by other branches.

OMB provides no formal training to the RMO program examiners regarding information systems management and related security issues. Each summer, OMB provides several days of seminars on issues of interest to examiners. However, only a few hours are devoted to topics handled by OIRA, including information resource management issues, such as system

development issues and security. Officials in the Information Policy and Technology Branch believe that ad hoc on-the-job learning is more effective in increasing the expertise of program examiners than a more formal program of training or awareness sessions would be. This is because the examiners can be overwhelmed by the volume of information available to them, and they are more likely to absorb information that is immediately useful. However, one branch chief said that there are few on-the-job learning opportunities regarding security issues because his branch devotes little attention to such issues.

Information Routinely Available for Oversight Is Limited

To effectively oversee and influence any activity, it is essential to have meaningful, reliable, and routinely available information on the operations being examined. However, the documented information that OMB routinely obtains on the design and effectiveness of agency information security programs varies significantly in quality, quantity, and usefulness.

Officials in OIRA's Information Policy and Technology Branch said that they routinely obtain annual internal control assessments required under the Federal Managers' Financial Integrity Act (FMFIA) and strategic information resource management plans. Since 1985, OMB Circular A-130, Appendix III, has directed agencies to review their sensitive systems at least every 3 years, certify the adequacy of security safeguards, and include identified weaknesses in the agencies' annual reports on internal controls required by FMFIA. Also, the Computer Security Act requires each agency to include a summary of its information security plan in its strategic information resource management plan that it submits annually to OMB. However, these documents vary significantly in level of detail and were often of little value for oversight purposes. Our review found that the FMFIA reports tended to contain very cursory information that made it difficult to precisely understand the nature of the weakness reported. Similarly, most of the security program summaries were very brief, and, in most cases, they only described very general agency goals and policies, with little information on the effectiveness of the program or on planned improvements. Further, the reporting formats varied considerably among agencies.

The RMO branches that we met with said that they attempted to obtain whatever information was available on the programs they examined, in addition to the agency budget documents that were the starting point for their examinations. However, most RMO examiners said that they did not routinely seek out information on or review agency security programs and

that any investigation of security issues that they made was almost always prompted by issues raised by management or auditors.

Most examiners said that they relied primarily on inquiries of agency officials and related documentation in examining agency programs, including any security issues that they were aware of. However, they also said that they used audit reports, usually issued by agency inspectors general and by GAO. Several examiners noted that such audit reports were useful both in providing them an independent assessment of agency operations and in strengthening their ability to encourage agency actions. Also, several of the branches said that their examinations benefitted from good working relationships with agency inspector general officials, who would alert them to key inspector general reports and other issues. We found that, for the most part, at least one examiner in each of the branches we met with was familiar with the information security weaknesses that had been reported in inspector general, GAO, and FMFIA reports for their agencies. However, some examiners were unaware of related detailed reports that had been issued on these weaknesses.

Until recently, independent audits of information security practices were performed largely at the discretion of inspector general offices and GAO and in response to congressional interest. As a result, OMB analysts and examiners could not rely on such reports being routinely available. However, program examiners at some agencies said that they have begun to review annual audits performed under the CFO Act as a means of monitoring agency control weaknesses, including those related to information security. These audits are discussed further in chapter 4 of this report.

Opportunities for Improving Oversight Are Emerging

Two relatively new developments can serve to improve and facilitate OMB's ability to oversee and influence the effectiveness of agency information security programs. One is an expansion of independent information security reviews prompted by financial statement audits required under the CFO Act. Another is the recently established CIO Council, which can serve as a forum for addressing governmentwide information security issues and raising security awareness.

Financial Statement Audits Are a Growing Source of Information on the Effectiveness of Information Security Controls

Although Inspector General offices and GAO have reviewed information security at federal agencies on a selective basis for decades, audits performed under the CFO Act promise to make such independent audit information more routinely available at all major agencies. Generally, CFO Act audits are required to include an evaluation of the auditee's internal controls, including information security controls. Such evaluations can assist OMB and the Congress in their oversight roles and serve as useful tools for agency managers.

In the early 1990s, selected segments of federal operations became subject to annual financial statement audits by agency inspector general offices under the CFO Act. In 1994, this audit requirement was extended to all major federal entities by the Government Management Reform Act (Public Law 103-356). As a result, the percentage of federal expenditures that is audited has been steadily growing, and, by fiscal year 1997, about 98 percent will be covered by such audits.

The primary responsibility for monitoring information security programs rests with agency managers who must routinely assess their programs and adjust policies and practices as needed. However, independent audits, such as the CFO Act audits, can be useful to OMB because they provide an objective evaluation that may identify weaknesses that were overlooked by agency self assessments. For example, IRS did not report its information security weaknesses in its annual FMFIA report until after independent audits had identified the weaknesses.

Although the reviews of computer security controls associated with CFO Act audits pertain to financial management systems, they usually cover a significant portion of each agency's operations. This is because program and financial systems often are supported by common data centers and communications networks that are subject to the same general controls. For example, personnel responsible for making needed changes to software are likely to follow the same set of procedures for controlling

such changes regardless of whether they pertain to a financial or nonfinancial system. Similarly, the adequacy of a disaster recovery plan for a large data center is likely to affect the security of all of that center's operations—both financial and nonfinancial. Also, program management systems often are the source of many detailed financial transactions and, therefore, are included in the auditor's review.

However, there are significant aspects of some agencies' operations involving sensitive computerized data that are not likely to be covered by financial statement audits. Examples include medical records and certain types of data supporting law enforcement operations. For this reason, it is important for OMB, as well as agency managers, to coordinate their reviews of CFO Act audit reports and their reviews of other information security assessments, such as self assessments conducted in accordance with FMFIA and OMB Circular A-130. When viewed together, these audits and assessments may provide a more comprehensive view of agency information security and allow OMB and agency officials to identify gaps in review coverage.

The awareness and use of CFO Act audit reports as a means of identifying information security weaknesses varied among the OMB analysts and examiners that we spoke with. This is understandable since audits of many agency programs have not been required until recently, and the routine availability of annual financial audit reports is relatively new. OIRA officials told us that they had not viewed these reports as a source of information on agency compliance with federal policies, because they did not realize that information security reviews were generally included in financial statement audits. However, they said that in the future, they would obtain CFO audit reports from OMB's Office of Federal Financial Management, where they are routinely received from agencies. The awareness of RMO program examiners was mixed. Most were aware of the CFO audit reports that affected the programs they were responsible for examining. However, a few were unaware of significant information security problems that had been reported.

New CIO Council Can Address Governmentwide Issues and Increase Awareness

Another recent development that can facilitate OMB's oversight is the recently established CIO Council. The Council, established in July 1996 through Executive Order, is intended to be "the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources." In this regard it is to support implementation of the Paperwork Reduction Act of 1995 and the Information Technology Management

Reform Act of 1996. It is chaired by OMB's Deputy Director for Management, and its membership includes CIOs from all major federal agencies.

The senior information resource managers that we spoke with and officials at OIRA agreed that the Council would be an appropriate forum for addressing information security issues and raising awareness governmentwide. However, officials at two agencies expressed their opinions that to be effective, the Council must take an active role in addressing problems, such as security, and go beyond just promoting awareness and sharing information.

With the support of the CIO Council and OMB, CIOs at individual agencies can raise the awareness of senior program officials to information security risks and serve as an important link between technical staff, who understand technical system and telecommunications vulnerabilities, and program managers, who understand the vulnerabilities associated with program activities, such as the risks of making inappropriate payments or inappropriately disclosing personal data on individuals. In addition, the CIOs can work together to identify and initiate efforts that benefit all of their agencies. Such efforts could include developing training programs, identifying best practices, and establishing interagency teams to review information security programs in multiple agencies.

Conclusions, Recommendations, and Agency Comments and Our Evaluation

While agencies are moving toward greater reliance on computers and electronic data to improve operations, recent reports indicate that many are not adequately addressing the associated risks. Most importantly, these agencies have not instituted security programs that are the foundation for ensuring that specific control techniques are appropriately selected and effectively implemented. The potential risks and related management challenges will increase as reliance on networked systems and electronic data increases and as more sophisticated control techniques become available. For this reason, it is important that OMB and agencies move promptly to increase senior management awareness of this problem and institute effective programs for managing these risks.

Implementing effective information security programs is primarily the responsibility of managers at individual federal agencies, since they are the most familiar with program risks and they have the ability to bring resources to bear where they will be most effective. However, OMB is responsible for overseeing these activities. OMB could strengthen its ability to fulfill this role if (1) it obtained more concise and meaningful information on the design of agency security programs and (2) RMO program examiners—the individuals with the most detailed understanding of agency operations—were more familiar with information security issues and did not have to depend as much on OIRA's limited staff for assistance.

Recommendations

To improve its oversight capability, it is important that OMB capitalize on every opportunity to leverage its resources and take advantage of all available information on agency information security practices. Some opportunities, including the increased number of annual financial statement audit reports and the recently established CIO Council, are already emerging as potential aids in overseeing and improving agency information security programs. However, there are additional steps that OMB can take to ensure that these opportunities are exploited and to increase the expertise of its staff. In this regard, we recommend that the Director of OMB take the following actions:

- Advocate and promote the CIO Council's adoption of information security as one of its top priorities and development of a strategic plan for (1) increasing awareness of the importance of information security, especially among senior agency executives, and (2) improving information security program management governmentwide. Initiatives that the CIO Council should consider incorporating in its strategic plan include

  - 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 using interagency teams of reviewers;
  - 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.
- Direct the Office of Information and Regulatory Affairs, the Office of Federal Financial Management, and the Resource Management Offices to (1) supplement their current reviews of audit reports to include reviewing audits conducted under the CFO Act in order to identify any findings related to information security and (2) use this information, in conjunction with reports on agency self assessments, to assist in proactively monitoring the scope of such reviews and the effectiveness of agency information security practices.
- Encourage the development of improved sources of information with which to monitor compliance with OMB's guidance and the effectiveness of agency information security programs. This could include engaging assistance from private contractors or others with appropriate expertise, such as federally funded research and development centers.[1]
- Direct the Office of Information and Regulatory Affairs to develop and implement a program for increasing 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.

Agency Comments and Our Evaluation

In written comments on a draft of this report, OMB agreed that information security is an important management issue and stated that certain of the report's recommendations are meritorious. In particular, OMB said that it will encourage the CIO Council to adopt information security as one of its top priorities and that it will review (1) the training and related materials

[1]Federally funded research and development centers are organizations sponsored by federal agencies to meet special research needs. The centers are operated by educational institutions, nonprofit organizations, and industrial firms.

provided to program examiners and (2) the availability of improved sources of information. However, OMB disagreed with the report's tone, which it characterized as suggesting "that OMB has not been dedicating sufficient resources in the past to overseeing the agencies' information security activities, and that therefore OMB in the future should dedicate more of its resources to this objective." In addition, OMB stated its concern that the report overemphasizes OMB's role and that this could distract federal agencies from their responsibilities as the primary managers of federal information security.

We agree that agency managers are primarily responsible for information security. Our audit efforts related to information security over the past few years have focused almost exclusively on individual agency practices, and we have made dozens of related recommendations to agency officials. Thirty products resulting from this work and containing these recommendations are listed at the end of this report. The results of this work led us to identify a pattern of governmentwide information security weaknesses.

In light of the pattern of weaknesses that we have identified and the increasing importance of information security in virtually every aspect of federal operations, OMB has a vital leadership role to play in promoting and overseeing agency security practices. This role was recently reemphasized in the Information Technology Management Reform Act of 1996 and in revisions to the Paperwork Reduction Act, which together explicitly outline OMB's responsibilities for overseeing agency practices regarding information privacy and security. Information security has become a consideration in the management of virtually every major federal program and in billions of dollars in annual information technology investment decisions. For these reasons, we believe that information security, as well as other information management issues, merits a high priority relative to other budget and management issues.

In this regard, our recommendations are focused primarily not on increasing the amount of OMB resources but on increasing the impact of OMB's current resources by taking advantage of newly available audit information, discussed in chapter 4, and by expanding staff expertise. These actions, at a minimum, are needed to help address growing concerns over the adequacy of federal information security. We also believe that periodic oversight reviews of agency information security programs would be beneficial but that such reviews could be performed

by interagency teams under the auspices of the OMB-chaired CIO Council, as we suggest in chapter 4.

Comments From the Office of Management and Budget

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

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

DEPUTY DIRECTOR
FOR MANAGEMENT

AUG 22 1996

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

Dear Mr. Dodaro:

This letter is in response to your letter of July 10, 1996, which forwarded copies of a draft GAO report entitled, "Information Security: Opportunities for Improved OMB Oversight of Agency Practices," and asked for our comments prior to its release. We appreciate the opportunity to comment on the draft report.

The draft report finds that: (1) information security weaknesses are widespread, (2) OMB's central policy has been updated, (3) OMB monitoring of agency practices has been uneven, (4) OMB's information for oversight is limited, and (5) the chief information officers (CIO) Council and Financial Audit reports offer opportunities for improved oversight.

The report recommends that OMB: (1) promote adoption of and action on information security as one of the top priorities of the CIO Council, (2) supplement current reviews of audit reports to include reviewing audits conducted under the Chief Financial Officers Act and use the information to proactively monitor the effectiveness of agency practices, (3) encourage the development of improved sources of information to monitor compliance with OMB's guidance, and (4) implement a program to increase program examiners' understanding of information security management issues and implications. The report contains no recommendations for agencies.

We appreciate the considerable effort that GAO has devoted to this study, and believe information security is an important management issue. Although certain of the draft report's recommendations are meritorious, we must nevertheless disagree with its overriding tone. The draft report strongly suggests that OMB has not been dedicating sufficient resources in the past to overseeing the agencies' information security activities, and that therefore OMB in the future should dedicate more of its resources to this objective. While OMB's information security oversight role is an important one, it remains only one of OMB's several information policy oversight responsibilities, which in turn comprise only one part of OMB's overall budget and management responsibilities.

See comment 1.

See comment 1.

OMB recently revised its Circular A-130, Appendix III, "Security of Federal Information Resources" in order to assist agencies in their efforts to improve information security. We are pleased that Federal agencies are finding it useful in improving the security of their systems. While the CIO Council will set its own agenda, we will encourage the Council to adopt information security as one of its top priorities. We are also reviewing the training and related materials we provide program examiners to improve their awareness of the importance of information security in agency operations and of the availability of improved sources of information.

See comment 2.

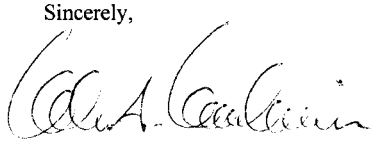
Given these activities, and while we are certainly open to suggestions for improving our oversight activities, we do not believe that a significant expansion of OMB's activities in the information security realm is warranted at this time. In particular, we do not believe it would be a prudent use of OMB's limited resources to take on the responsibility of doing more frequent or in-depth compliance reviews of each individual agency's information security practices. Ensuring an agency's compliance must necessarily be the primary responsibility of the agency itself.

See comment 3.

We would observe that, although three of the four objectives of the GAO review focussed directly on agency practices and a variety of report weaknesses were discussed, the report makes no recommendations for agency actions. 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 Federal agencies from their primary responsibility for assuring information security.

We share your concern that Federal information be adequately secure. We also recognize the important responsibility of OMB to oversee that security and appreciate the opportunity to comment on the draft report. We look forward to future opportunities to work with you and your staff on these important matters.

Sincerely,



John A. Koskinen

The following are GAO's comments on OMB's letter of August 22, 1996.

GAO Comments

1. Discussed in the "Agency Comments and Our Evaluation" sections in the executive summary and at the end of chapter 5.

2. We do not recommend that OMB's limited staff be used to perform in-depth compliance reviews at individual agencies. However, we believe that OMB does have responsibility for overseeing compliance with the guidance it has issued and that it should work to improve its ability to do so. The report recommends that OMB (1) take advantage of the growing amount of audit information on information security that is being prompted by CFO Act audits at individual agencies and (2) encourage the development of improved sources of information with which to monitor compliance with OMB's guidance. We also believe that periodic oversight reviews of agencies' information security programs would be beneficial but that such reviews could be performed by interagency teams under the auspices of the OMB-chaired CIO Council, as we suggest in chapter 4.

3. The report does not contain recommendations to agencies because numerous such recommendations have already been included in other GAO products. Thirty of these products, most of which contain recommendations to individual agencies, are listed at the end of this report. Other reports on information security have been issued by agency inspectors general, as discussed in chapter 2. We believe that the audit emphasis on information security will continue, in part as a result of the CFO Act audits and in part due to growing concerns regarding security in a networked computer environment. Such audits will serve as continuing reminders to federal agency managers of their information security responsibilities.

Major Contributors to This Report

Accounting and Information Management Division, Washington, Dc

Jean L. H. Boltz, Assistant Director
Richard L. Sumner, Information Systems Analyst
Ona Noble, Information Systems Analyst

Related GAO Products

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 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).

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

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1994 and 1993 (GAO/AIMD-96-22, February 26, 1996).

Financial Management: Challenges Facing DOD in Meeting the Goals of the Chief Financial Officers Act (GAO/T-AIMD-96-1, November 14, 1995).

Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/ AIMD-95-141, August 4, 1995).

Financial Audit: Resolution Trust Corporation's 1994 and 1993 Financial Statements, (GAO/AIMD-95-157, June 22, 1995).

Federal Family Education Loan Information System: Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data (GAO/AIMD-95-117, June 12, 1995).

Department of Energy: Procedures Lacking To Protect Computerized Data (GAO/AIMD-95-118, June 5, 1995).

Financial Management: Control Weaknesses Increase Risk of Improper Navy Civilian Payroll Payments (GAO/AIMD-95-73, May 8, 1995).

Information Superhighway: An Overview of Technology Challenges (GAO/AIMD-95-23, January 23, 1995).

Management Reform: Implementation of the National Performance Review's Recommendations (GAO/OCG-95-1, December 5, 1994).

Information Superhighway: Issues Affecting Development (GAO/RCED-94-285, September 30, 1994).

Financial Audit: Federal Deposit Insurance Corporation's Management Letter as of December 31, 1993 (GAO/AIMD-94-160ML, August 29, 1994).

IRS Automation: Controlling Electronic Filing Fraud and Improper Access to Taxpayer Data (GAO/T-AIMD/GGD-94-183, July 19, 1994).

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1993 and 1992 (GAO/AIMD-94-131, June 30, 1994).

Financial Management: CFO Act Is Achieving Meaningful Progress (GAO/T-AIMD-94-149, June 21, 1994).

Financial Audit: Examination of Customs' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-119, June 15, 1994).

Financial Audit: Examination of IRS' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-120, June 15, 1994).

HUD Information Resources: Strategic Focus and Improved Management Controls Needed (GAO/AIMD-94-34, April 14, 1994).

Financial Audit: Federal Deposit Insurance Corporation's Internal Controls as of December 31, 1992 (GAO/AIMD-94-35, February 4, 1994).

Financial Management: Strong Leadership Needed to Improve Army's Financial Accountability (GAO/AIMD-94-12, December 22, 1993).

Communications Privacy: Federal Policy and Actions (GAO/OSI-94-2, November 4, 1993).

IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, September 22, 1993).

Document Security: Justice Can Improve Its Controls Over Classified and Sensitive Documents (GAO/GGD-93-134, September 7, 1993).

National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information (GAO/T-GGD-93-41, July 28, 1993).

Financial Audit: Examination of the Army's Financial Statements for Fiscal Years 1992 and 1991 (GAO/AIMD-93-1, June 30, 1993).

Computer Security: DEA Is Not Adequately Protecting National Security Information (GAO/IMTEC-92-31, September 30, 1992).

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 6015
Gaithersburg, MD 20884-6015

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 (301) 258-4066, or TDD (301) 413-0006.

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

PRINTED ON RECYCLED PAPER

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