

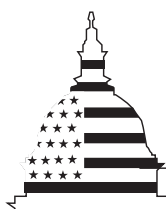
GAO

Report to the Chairman, Subcommittee
on Government Management,
Information and Technology, Committee
on Government Reform, House of
Representatives

September 2000

INFORMATION SECURITY

Serious and Widespread Weaknesses Persist at Federal Agencies



G A O

Accountability * Integrity * Reliability

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 01092000	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) GAO		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms "IATAC COLLECTION"		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 37		

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 9/1/00		3. REPORT TYPE AND DATES COVERED Report
4. TITLE AND SUBTITLE Information Security: Serious and Widespread Weaknesses persist at Federal Agencies			5. FUNDING NUMBERS	
6. AUTHOR(S) GAO				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) Congressional report on computer security grading the US Federal Government Agencies on how vulnerable are their computers. This subcommittee is releasing its first report card on the status of computer security at the executive branch departments and agencies. These grades are based on self-reported agency information in addition to the results of audits conducted by the General Accounting Office and agency Inspectors General. This is the first time such government -wide information has ever been compiled.				
14. SUBJECT TERMS Information Security			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	



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

**Accounting and Information
Management Division**

B-286154

September 6, 2000

The Honorable Stephen Horn
Chairman, Subcommittee on Government Management,
Information and Technology
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

This report responds to your July 28, 2000, request that we summarize the results of recent information security audits at federal agencies. Like other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to help avoid disruptions in critical operations, data tampering, fraud, and inappropriate disclosures of confidential information.

This report summarizes audit findings for the 24 federal agencies that were included in a similar review that we reported on in September 1998—agencies that, during fiscal year 1999, accounted for almost 99 percent of federal outlays. In our 1998 report, we concluded that significant computer security weaknesses had been reported for each of those agencies and that, as a result, critical federal operations and assets were at risk.¹

In accordance with your request, our objectives were to (1) analyze and summarize information security weaknesses identified in audit reports issued from July 1999 through August 2000 and compare our findings with similar information that we reported in September 1998, (2) identify examples of weaknesses and the related risks at selected individual agencies, and (3) identify the most significant types of weaknesses in each of six categories of general controls that we used in our analysis. The agency audit reports we analyzed, most of which are referenced throughout this report, were produced primarily by us and agency inspectors general (IG).

¹*Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

Results in Brief

Evaluations of computer security published since July 1999 continue to show that federal computer security is fraught with weaknesses and that, as a result, critical operations and assets continue to be at risk. As in 1998, our current analysis identified significant weaknesses in each of the 24 agencies covered by our review. Since July 1999, the range of weaknesses in individual agencies has broadened, at least in part because the scope of audits being performed is more comprehensive than in prior years. While these audits are providing a more complete picture of the security problems agencies face, they also show that agencies have much work to do to ensure that their security programs are complete and effective.

The weaknesses identified place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections, and weaknesses at the Department of Defense increase the vulnerability of various military operations that support the department's war-fighting capability. Further, information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure. For example, in 1999, a Social Security Administration employee pled guilty to unauthorized access of the administration's systems. The related investigation determined that the employee had made many unauthorized queries, including obtaining earnings information for members of the local business community.

For most agencies, the weaknesses reported covered the full range of computer security controls. For example, security program planning and management were inadequate. Physical and logical access controls also were not effective in preventing or detecting system intrusions and misuse. In addition, software change controls were ineffective in ensuring that only properly authorized and tested software programs were implemented. Further, duties were not adequately segregated to reduce the risk that one individual could execute unauthorized transactions or software changes without detection. Finally, sensitive operating system software was not adequately controlled, and adequate steps had not been taken to ensure continuity of computerized operations.

We and agency inspectors general have made scores of recommendations to agencies regarding specific steps they should take to make their security programs more effective. Most agencies have heeded these recommendations and taken at least some corrective actions. However,

more needs to be done, especially in the area of security program planning and management, which involves instituting routine risk management activities aimed at ensuring that risks are understood, that appropriate controls are implemented commensurate with risk, and that these controls operate as intended.

Background

Dramatic increases in computer interconnectivity, especially in use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of other individuals and groups.

However, in addition to its benefits, this widespread interconnectivity poses significant risks to our computer systems and, more importantly, to the critical operations and infrastructures they support, such as telecommunications; power distribution; national defense, including the military's warfighting capability; law enforcement; government services; and emergency services. The same factors that benefit operations—speed and accessibility—if not properly controlled, also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on these operations from remote locations for purposes of fraud or sabotage, or for other malicious or mischievous purposes. Disruptions caused by recent virus attacks, such as the ILOVEYOU virus in May 2000 and 1999's Melissa virus, have illustrated the potential for damage that such attacks hold.² In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected.

²*Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000). *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000). *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

Government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan Horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, or degrade the integrity of and deny access to data. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, there is a greater likelihood that information attacks will threaten vital national interests.

While complete summary data are not available because many computer security incidents are not reported, the number of incidents that are reported is growing. For example, the number of reported incidents handled by Carnegie-Mellon University's CERT Coordination Center³ has increased from 1,334 in 1993 to 8,836 during the first two quarters of 2000. Similarly, the Federal Bureau of Investigation reports that its case load of computer intrusion-related cases is more than doubling every year. The fifth annual survey conducted by the Computer Security Institute in cooperation with the FBI found that 70 percent of respondents (primarily large corporations and government agencies) had detected serious computer security breaches within the last 12 months and that quantifiable financial losses had increased over past years.⁴

Our previous analyses have shown that federal agency systems were not being adequately protected from these threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September 1996, we

³Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.

⁴*Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey*, The Computer Security Institute, March 2000.

reported that serious weaknesses had been reported for 10 of the largest 15 federal agencies.⁵ In that report we concluded that poor information security was a widespread federal problem with potentially devastating consequences, and, in 1997 and 1999 reports to the Congress, we identified information security as a high-risk issue.⁶ In 1998, we analyzed audit results for 24 of the largest federal agencies and reported that all of them had significant information security weaknesses.⁷

The primary responsibility for implementing adequate security lies with individual agencies. Officials in these agencies are most familiar with the agency programs and assets that are at risk, and, therefore, they are in the best position to (1) determine what operations and assets merit the strongest protection and control and (2) ensure that security programs are effective on an ongoing basis. Accordingly, improvements must be implemented at the individual agency level.

Centrally directed governmentwide efforts to improve federal information security are also important to provide central policy direction and address issues that affect multiple agencies. Several such efforts are underway, many as part of broader efforts to protect our nation's critical computer-support infrastructures. Most recently, in January 2000, the President issued the National Plan for Information Systems Protection,⁸ which called for new initiatives to strengthen the nation's defenses against threats to public and private sector critical information systems. In addition, the federal Chief Information Officers Council and others have several projects underway that are intended to promote and support information security improvements.

⁵*Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

⁶*High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997), *High-Risk Series: An Update* (GAO/HR-99-1, January 1999).

⁷*Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

⁸*Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*, released January 7, 2000, The White House.

Weaknesses Remain Pervasive

As in our 1998 analysis, audit reports issued since July 1999 identified significant information security weaknesses in each of the 24 agencies covered by our analysis. Also, as in 1998, weaknesses were reported in all six major areas of “general controls” that we used to categorize them. General controls are the policies, procedures, and technical controls that apply to all or a large segment of an entity’s information systems and help ensure their proper operation. These weaknesses placed a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they placed an enormous amount of highly sensitive data, much of it on individual taxpayers and beneficiaries, at risk of inappropriate disclosure.

Table 1 provides an overview of the types of weaknesses reported throughout the government, as well as the gaps in audit coverage.

Table 1: Areas of Information Security Weakness Reported for 24 Federal Agencies

General control area	Number of agencies					
	Significant weakness identified		No significant weakness identified		Area not reviewed	
	1998	2000	1998	2000	1998	2000
Entitywide security program planning and management	17	21	0	0	7	3
Access controls	23	24	0	0	1	0
Application software development and change controls	14	19	4	2	6	3
Segregation of duties	16	17	1	3	7	4
System software controls	9	18	0	0	15	6
Service continuity controls	20	20	0	1	4	3

As in 1998, the most widely audited area and the area where weaknesses were most often identified was access controls. Weak controls over access to sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today’s increasingly interconnected computing environment, poor access controls can expose an agency’s information and operations to attacks from remote

locations all over the world by individuals with minimal computer and telecommunications resources and expertise.

Many problems were also identified in the area of entitywide security program planning and management—an area that is fundamental to the appropriate selection and effectiveness of the other categories of controls. Security program planning and management cover a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

One notable change since September 1998 is that the scope of audit work performed has expanded to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to identification of additional areas of weakness at some agencies and an overall increase in the number of agencies with significant weaknesses identified in five of the six general control categories. While these increases in reported weaknesses are disturbing, they do not necessarily mean that information security at federal agencies is getting worse. It is more likely that they show that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the numbers in table 1 leave no doubt that serious weaknesses are pervasive.

As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified. Most of the audits used to develop table 1 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at other agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits used to develop this table may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluating systems supporting nonfinancial operations. In response to congressional interest, during fiscal year 1999 and 2000, we expanded our audit focus to cover a wider range of nonfinancial operations, a trend that is likely to continue.

Examples of Weaknesses at Individual Agencies Highlight Risks to Operations, Assets, Confidentiality

To understand the significance of the weaknesses summarized in table 1, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Reported weaknesses and the significant risks they pose to critical federal operations are described below.

Department of the Treasury

The Department of the Treasury (which includes the Internal Revenue Service; U.S. Customs Service; Bureau of the Public Debt; Financial Management Service; and Bureau of Alcohol, Tobacco, and Firearms) relies on computer systems to process, collect or disburse, and account for over \$1.8 trillion in federal receipts and payments annually. In addition, the department's computers handle enormous amounts of highly sensitive data associated with taxpayer records, law enforcement operations, and support operations critical to financing the federal government, maintaining the flow of benefits to individuals and organizations, and controlling imports and exports.

Although protecting these operations and assets is essential to the welfare of our nation, in February 2000, the Treasury IG reported that absence of effective general controls over computer-based financial systems at certain Treasury components continued to be a material weakness in the department's internal controls.⁹ The IG report explained that this absence of controls makes the department vulnerable to losses, fraud, delays, and interruptions in service. In addition, it compromises the integrity and reliability of the department's information systems and data.

Weaknesses for specific Treasury bureaus include the following.

- In October 1999, we reported that pervasive computer security weaknesses at Treasury's Financial Management Service placed billions of dollars of payments and collections at significant risk of loss or fraud, vast amounts of sensitive data at risk of inappropriate disclosure, and

⁹Report on the Department of the Treasury's Fiscal Year 1999 Financial Statements (OIG-00-056, February 29, 2000).

critical computer-based operations at risk of serious disruption.¹⁰ These weaknesses affected a wide array of information systems that the Financial Management Service uses in its role as the government's central financial manager, disbursing, and collection agency.

- In February 2000, we reported that significant weaknesses in the Internal Revenue Service's (IRS) computer security controls continued to place taxpayer and other data in IRS' automated systems at serious risk of unauthorized disclosure, modification, or destruction.¹¹ Specifically, IRS continued to have serious weaknesses with general controls designed to protect computing resources such as networks, computer equipment, software programs, data, and facilities from unauthorized use, modification, loss, and disclosure. IRS did not always (1) effectively implement controls to prevent, limit, or detect access to computing resources, (2) adequately segregate system administration and security administration responsibilities, (3) optimally configure system software to ensure the integrity of system programs, files, and data, (4) sufficiently plan or test the activities required to restore critical business systems when unexpected events occur, and (5) routinely monitor key networks and systems to identify unauthorized activities and inappropriate system configurations.
- In February 2000, the Treasury IG reported significant deficiencies in the Customs Service's ability to provide for the timely restoration of mission-critical systems that could impair Customs' ability to respond effectively to a disruption in operations.¹² The Treasury IG determined that Customs had not established a framework to assess risk, developed and implemented effective security procedures, or monitored the effectiveness of these procedures on a continuous basis. In addition, the IG identified weaknesses in Customs' logical access controls over its data files, application programs, and computer-related facilities, equipment, and infrastructure. Weaknesses in controls over computer-based financial systems makes Customs vulnerable to losses, delays, or

¹⁰ *Financial Management Service: Significant Weaknesses in Computer Controls* (GAO/AIMD-00-4, October 4, 1999).

¹¹ *Financial Audit: IRS' Fiscal Year 1999 Financial Statements* (GAO/AIMD-00-76, February 29, 2000). Also see *IRS Systems Security: Although Improvements Made, Tax Processing Operations and Data Still at Serious Risk* (GAO/AIMD-99-38, December 14, 1998).

¹² *Report on the Department of the Treasury's Fiscal Year 1999 Financial Statements* (OIG-00-056, February 29, 2000).

interruptions in service, and compromise the integrity and reliability of the information systems and data.

Numerous recommendations have been made to Treasury bureaus over the years to correct these weaknesses, and many corrective actions are underway. In particular, IRS has made notable progress in improving computer security at its facilities and has corrected a significant number of the computer security weaknesses identified in our previous reports. Also, IRS has established a servicewide computer security management program that should, when fully implemented, help the agency effectively manage its security risks.

Department of Defense

The Department of Defense (DOD) relies on a vast and complex computerized information infrastructure to support virtually all aspects of its operations, including strategic and tactical operations, weaponry, intelligence, and security. This reliance extends to its business operations that support the department, including financial management.

Evaluations of the security of DOD systems since July 1999 have continued to identify weaknesses that could seriously jeopardize operations and compromise the confidentiality, integrity, or availability of sensitive information. In August 1999, we reported that serious weaknesses in DOD information security continued to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data.¹³ These weaknesses impaired DOD's ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its systems is properly authorized, tested, and functioning as intended, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous DOD functions—including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll—had already been adversely affected by system attacks or fraud. In May 1996, we had reported that attackers had stolen, modified, and destroyed both data and software at DOD and installed “back doors” that circumvented normal system protection and allowed attackers

¹³*DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999).

unauthorized future access.¹⁴ They had also shut down and crashed entire systems and networks.

In our August 1999 report, we stated that some corrective actions had been initiated in response to recommendations we made in 1996 to address pervasive information security weaknesses in DOD. However, progress in correcting specific control weaknesses identified in 1996 and in previous reviews had been inconsistent across the various DOD components. Although many factors contribute to these weaknesses, audits by us and the DOD IG have found that an underlying cause of weak information security is poor management of security programs. In August 1999, we reiterated this finding, as well as our recommendation that DOD take steps to strengthen departmentwide security program management.

In May 2000, we testified that the preliminary results of a recent review of the department's financial management systems showed that serious weaknesses in access controls and systems software continued to exist.¹⁵ During that review, we gained access to sensitive information through a file that was publicly available over the Internet and, without valid user authentication, gained access to employees' social security numbers, addresses, and pay information, as well as budget, expenditure, and procurement information on projects. At the close of this review, the responsible DOD component was taking corrective actions.

DOD has been taking steps to improve the department's information security. Notably, the department has established the (1) Defense-wide Information Assurance Program under the jurisdiction of the DOD Chief Information Officer and (2) Joint Task Force for Computer Network Defense to monitor DOD computer networks and defend against hacker attacks and other unauthorized access. We are currently reviewing these efforts.

Department of Energy

Information technology is essential to the Department of Energy's (DOE) scientific research mission, which is supported by a large and diverse set of computing systems, including very powerful supercomputers, located at

¹⁴*Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (GAO/AIMD-96-84, May 22, 1996).

¹⁵*Department of Defense: Progress in Financial Management Reform* (GAO/T-AIMD/NSIAD-00-163, May 9, 2000).

DOE laboratories across the nation. Much of the research conducted at the laboratories is unclassified, and DOE officials have had to struggle to convince their user community that security threats are real and that effective security measures can be implemented that will not significantly constrain the openness they require to do scientific research.

In June 2000, we reported that computer systems at DOE laboratories supporting civilian research had become a popular target of the hacking community with the result that the threat of attacks had grown dramatically in recent years.¹⁶ We further noted that because of security breaches, several laboratories had been forced to temporarily disconnect their networks from the Internet, disrupting the laboratories' ability to do scientific research for up to a full week on at least two occasions.

In our report, we stated that a major contributing factor to the existence of DOE's security vulnerabilities was that the department did not have an effective program for managing information technology security consistently throughout the department. Specifically, during our review, we found that DOE had not (1) prepared federally required security plans, (2) effectively identified and assessed information security risks, (3) provided adequate policy guidance on what information was appropriate for public Internet access, (4) effectively overseen implementation of computer security at the laboratories, and (5) fully and consistently reported security incidents.

We recommended that the Secretary of Energy take specific actions to strengthen the management of the department's unclassified computer security program. The department generally agreed with our recommendations and provided information on the actions it is taking.

Department of Health and Human Services

In February 2000, the Department of Health and Human Services (HHS) IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.¹⁷ Most significant were weaknesses associated with the department's Health Care Financing Administration (HCFA), which, according to its reports,

¹⁶*Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/AIMD-00-140, June 9, 2000).

¹⁷*Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1999*, A-17-99-00002, February 2000.

was responsible, during fiscal year 1999, for processing health care claims for over 39.5 million beneficiaries and outlays of \$299 billion—17.5 percent of total federal outlays.

HCFA relies on extensive data processing operations at its central office to maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and to process all payments for managed care. In fiscal year 1999, managed care payments totaled about \$37 billion. HCFA also relies on Medicare contractors, who use multiple shared systems to collect and process personal health, financial, and medical data associated with about 870 million Medicare claims annually.

The IG's recent report identified many general control weaknesses associated with computer controls at HCFA's central office, Medicare contractors, and the contractors' shared systems. At the central office, weaknesses were identified in access controls, application software development and change controls, entitywide security program planning and management, and operating system software controls. At Medicare contractors, weaknesses were identified in these same areas plus weaknesses in segregation of duties and service continuity. Such weaknesses increase the risk of (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper Medicare payments, or (4) disruption of critical operations. The report included many recommendations for addressing the identified weaknesses.

Both HCFA and the Medicare contractors have taken steps to address previously reported weaknesses. In particular, the HCFA central office is planning for additional security software to restrict access to sensitive Medicare databases. In addition, HHS has recognized the need to protect the security of information technology systems and the data contained in them, and the department continues to revise security policies and guidance and to require each major operating division to develop and implement corrective action plans to address unresolved weaknesses. However, serious weaknesses persist.

Social Security Administration

The Social Security Administration (SSA) relies on extensive information processing resources to carry out its operations, which, for 1999, included payments that totaled \$410 billion to more than 50 million beneficiaries, many of whom rely on the uninterrupted flow of monthly payments to meet their basic needs. This represents about 25 percent of the \$1.7 trillion in

federal expenditures. The administration also issues social security numbers and maintains earnings records and other personal information on virtually all U.S. citizens. The public depends on SSA to protect trust fund revenues and assets from fraud and to protect sensitive information on individuals from inappropriate disclosure. According to SSA, no other public program or public-service entity directly touches the lives of so many people.

In November 1999, the SSA IG reported that SSA's systems environment remained threatened by weaknesses in several components of its information protection control structure.¹⁸ The general areas where weaknesses were noted were (1) entitywide security program planning and management and associated weaknesses in developing, implementing, and monitoring local area networks and distributed systems security, (2) SSA's mainframe computer security and operating system configuration, (3) physical access controls at nonheadquarters locations, and (4) certification and accreditation of certain general support and major application systems. In addition, the IG reported that SSA needed to complete and fully test its plan for maintaining continuity of operations.

According to the IG, until corrected, the weaknesses will continue to increase the risks of unauthorized access to, modification, or disclosure of sensitive SSA information. These, in turn, increase the risks that data or SSA Trust Fund resources could be lost and that the privacy of information associated with SSA's enumeration, earnings, retirement, and disability processes and programs could be compromised.

Such weaknesses might allow an individual or group to fraudulently obtain payments by creating fictitious beneficiaries or increasing payment amounts. Similarly, an individual or group might secretly obtain sensitive information and sell or otherwise use it for personal gains. In 1999, a SSA employee pled guilty to unauthorized access of SSA's systems from 1993 through November 1997 and, as part of a plea agreement, was required to pay \$4,658 to SSA in restitution and resign from the agency. This case was initiated based on an anonymous tip alleging that the SSA employee had accessed SSA records. The IG confirmed the unauthorized access and learned during the investigation that the SSA employee had made many other unauthorized queries, including obtaining earnings information for

¹⁸ *Social Security Accountability Report for Fiscal Year 1999*, November 18, 1999.

members of the local business community, such as a bank president, a pharmacist, a physician, an attorney, and a psychologist.

In separate letters issued to SSA management, the IG and its contractor made recommendations to address the weaknesses reported in November 1999. SSA agreed with the majority of the recommendations in the SSA IG's report and agreed to develop related corrective action plans.

Environmental Protection Agency

The Environmental Protection Agency (EPA) relies on its computer systems to collect and maintain a wealth of environmental data under various statutory and regulatory requirements. EPA makes much of its information available to the public through Internet access in order to encourage public awareness and participation in managing human health and environmental risks and to meet statutory requirements. EPA also maintains confidential data from private businesses, data of varying sensitivity on human health and environmental risks, financial and contract data, and personal information on its employees. Consequently, EPA's information security program must accommodate the often competing goals of making much of its environmental information widely accessible while maintaining data integrity, availability, and appropriate confidentiality.

In July 2000, we reported serious and pervasive problems that essentially rendered EPA's agencywide information security program ineffective.¹⁹ Our tests of computer-based controls concluded that the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses. Our report included over 100 recommendations for correcting specific control weaknesses and strengthening EPA's agencywide security program.

Of particular concern was that many of the most serious weaknesses we identified—those related to inadequate protection from intrusions through the Internet and poor security planning—had been previously reported to EPA management in 1997 by EPA's IG.²⁰ The negative effects of such

¹⁹*Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215, July 6, 2000).

²⁰*EPA's Internet Connectivity Controls*, Office of Inspector General Report of Audit (Redacted Version), September 5, 1997.

weaknesses are illustrated by EPA's own records, which show several serious computer security incidents since early 1998 that have resulted in damage and disruption to agency operations.

As a result of these weaknesses, EPA's computer systems and the operations that rely on these systems were highly vulnerable to tampering, disruption, and misuse from both internal and external sources. Moreover, EPA could not ensure the protection of sensitive business and financial data maintained on its larger computer systems or supported by its agencywide network.

EPA has acted to reduce the exposure of its systems and data and to correct the access control weaknesses we identified. Equally important are EPA's efforts to improve its security program planning and management—changes that are essential to sustaining the effectiveness of its access controls. Our July 2000 report stated that EPA's existing security program planning and management practices were largely a paper exercise that had done little to substantively identify, evaluate, and mitigate risks to the agency's data and systems. Accordingly, EPA's planned improvements will require a major adjustment in the way agency program and technical staff manage the agency's information security risks.

Department of Transportation

The Department of Transportation (DOT) consists of 11 operating administrations, including the U.S. Coast Guard, the Federal Highway Administration, the Federal Railway Administration, and the Federal Aviation Administration (FAA). To perform their diverse missions, the DOT operating administrations rely on complex infrastructures of computer hardware, software, and communications systems. At last count, DOT had over 600 mission-critical systems, including FAA air traffic control systems, Coast Guard search and rescue systems, and financial systems that track billions of federal dollars.

In July 2000, DOT's IG reported that reviews of a financial system and 13 network systems identified a general lack of background checks on contractor personnel and a lack of appropriate background checks on employees throughout DOT.²¹ The IG also found that the department's systems were vulnerable to unauthorized access by Internet users.

²¹*Interim Report on Computer Security* (FI-2000-108, July 13, 2000).

In addition, in December 1999, we reported that the FAA was not following sound personnel security practices and, as such, had increased the risk that inappropriate individuals may have gained access to its facilities, information, or resources.²² FAA's personnel security policy requires system owners and users to prepare risk assessments for all contractor tasks and to conduct background investigations for all contractor employees in high-risk positions. The policy requires more limited background checks for moderate- and low-risk positions. However, we found that FAA did not perform all the necessary risk assessments and was unaware of whether anyone had performed background searches on all of the contractor employees. Further, we found instances where background searches were not performed. For example, no background searches were performed on 36 mainland Chinese nationals who reviewed the source code of eight mission-critical systems.

In May 2000, we reported that FAA was making progress in implementing its personnel security policy but still needed to complete the required background searches for a substantial number of contractor employees.²³ We are continuing to evaluate these areas and FAA's overall computer security program.

Department of Veterans Affairs

The Department of Veterans Affairs (VA) relies on a vast array of computer systems and telecommunications systems to support its operations and store sensitive information the department collects in carrying out its mission. Such operations include financial management, health care delivery, and benefit payments.

In September 1998, we reported weaknesses that placed the systems that support these operations at risk of misuse and disruption.²⁴ In October 1999, we reported that VA systems continued to be vulnerable to

²²*Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, December 23, 1999).

²³*Computer Security: FAA Is Addressing Personnel Weaknesses, But Further Action Is Required* (GAO/AIMD-00-169, May 31, 2000).

²⁴*Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-98-175, September 1998).

unauthorized access.²⁵ Specifically, according to our and VA IG reports, VA had not adequately limited access of authorized users or effectively managed user identifications and passwords and had not properly segregated computer duties. VA's access control weaknesses were further compounded by ineffective procedures for overseeing and monitoring systems for unusual or suspicious access activities. These weaknesses placed sensitive information, including financial data and sensitive veteran medical data and benefit information at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. Accordingly, we provided the VA with over 75 recommendations aimed at correcting these problems. VA has recognized the significance of these problems, reporting information security as a material weakness in its Federal Managers' Financial Integrity Act (FMFIA) report for 1998 and 1999.

One reason for VA's continuing information system control problems is that the department had not implemented a comprehensive, integrated security management program. While VA officials had established a central security group and developed and partially implemented an information security program plan, they had not yet developed detailed guidance to ensure that key information security areas highlighted in our October 1999 report—assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls—were fully addressed and consistently implemented throughout the department. The department plans to implement additional security initiatives by May 2001 and establish a fully operational security program by January 2003.

Department of Agriculture

In July 1999, we reported that the Department of Agriculture's National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent or detect unauthorized changes to payroll and other payment data or computer software.²⁶ NFC is responsible for processing billions of dollars in payroll payments for hundreds of thousands of federal employees and maintaining records for the world's largest 401(k)-type program. Specifically, NFC had not sufficiently restricted access authority for legitimate users. In one instance, 86 users identifications had an access

²⁵*Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 1999).

²⁶*USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-99-227, July 30, 1999).

privilege that allows users to read and alter any data tape, including payroll files, regardless of other security software controls. In addition, 60 mainframe computer users had been granted privileges that allowed them to access sensitive operating system files, including audit trail information. Further, NFC had not adequately (1) established security policies and procedures that addressed all aspects of NFC's interconnected environment or (2) implemented a process to measure, test, and report on the effectiveness of computer controls.

In August 2000, the Department of Agriculture IG reported that, while the NFC had completed corrective actions on 31 of 35 technical weaknesses we had identified, 4 weaknesses, pertaining to logical access controls, had not been corrected. In addition, the IG found that NFC had not implemented an entitywide security program as we had recommended.²⁷

Other Federal Operations

- In June 2000, we testified that the Department of State, while taking several positive steps, had not adequately addressed previously reported access control and security program management weaknesses.²⁸ Our review found that State still needed to take steps to ensure that all audit recommendations and identified security vulnerabilities are addressed, expand its automated intrusion detection program, and further clarify agencywide security management responsibilities.
- In May 2000, based on a survey of 16 federal agencies, we reported that controls over changes to software for federal information systems as described in agency policies and procedures were inadequate.²⁹ Specifically, we found that in many cases (1) formally documented policies and procedures did not exist or did not meet the requirements of federal criteria, (2) oversight of contractors was inadequate, especially when software change functions were completely contracted out, and (3) background screenings of personnel involved in the software change process were not a routine security control. Such

²⁷ *Review of Corrective Actions Taken by the National Finance Center on General Accounting Office Recommendations in Report GAO/AIMD-99-195, dated July 30, 1999, Memorandum from USDA IG to USDA Chief Financial Officer, August 11, 2000.*

²⁸ *Foreign Affairs: Effort to Upgrade Information Technology Overseas Faces Formidable Challenges* (GAO/T-AIMD/NSIAD-00-214, June 22, 2000).

²⁹ *Information Security: Controls Over Software Changes at Federal Agencies* (GAO/AIMD-00-151R, May 4, 2000).

weaknesses increase the risks that untrustworthy and untrained individuals could have unrestricted access to software code, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. We suggested many remedies for the weaknesses we identified, and officials at many of the 16 agencies told us that they had begun to implement them.

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

The nature of agency operations and the related risks vary. However, as we reported in September 1998, there are striking similarities in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. The following sections describe each of the six areas of general controls and the specific weaknesses that were most widespread at the agencies covered by our analysis.

Entitywide Security Program Planning and Management

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

Despite the importance of this aspect of an information security program, poor security planning and management continues to be a widespread problem. As noted earlier, of the 21 agencies for which this aspect of security was reviewed, all had deficiencies. Many of these agencies had not developed security plans for major systems based on risk, had not documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, agencies (1) were not fully aware of the information security risks to their operations, (2) had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable, (3) had a false sense of security because they were relying on controls that were not effective, and (4) could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections, such as gates and guards, as well as logical controls, which are controls built into software that (1) require users to authenticate themselves through the use of secret passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can execute. Without adequate access controls, unauthorized individuals, including outside intruders and terminated employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users could unintentionally modify or delete data or execute changes that are outside of their span of authority.

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

Access controls were evaluated at all 24 of the agencies covered by our review, and significant weaknesses were reported for each of these 24, as evidenced by the following examples.

- Agencies had not implemented effective user account and password management practices to reduce the risk that accounts could be used to gain unauthorized system access. Examples include the following.
 - Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled.
 - Users did not periodically change their passwords.
 - Access was not promptly terminated when users either left the agency or adjusted when their responsibilities no longer required them to have access to certain files.
 - Inactive user identifications were not routinely identified and deleted. As a result, contractors and former employees who were no

longer associated with the agency could still read, modify, copy, or delete data, and employees who changed positions within an agency had access to files that were not needed in their new positions. At one agency, an individual no longer officially affiliated with the agency gained access to an agency computer and altered the access privileges, indicating a serious weakness in the agency's process for applying changes in personnel status to computer accounts. At another agency, individuals, mostly contractor employees, who were no longer working for the agency still retained access to agency systems, and some accounts were used after the individuals left agency employment. Also at this agency, 7,500 of 30,000 users were not deleted after 160 days of inactivity.

- Managers had not precisely identified access needs for individual users or groups of users. Instead, they had provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings.
- Access was not appropriately authorized and documented. For example, at one agency, 20,000 users had been provided access to one system without written authorization.
- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the capability to read sensitive production data, increasing the risk that sensitive information could be disclosed to unauthorized individuals. Also, at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs. At another agency, 74 user accounts had been granted privileges enabling them to change program code without supervisory review or approval.
- User activity was not adequately monitored to deter and identify inappropriate actions. At one agency, much of the activity associated with our intrusion testing was not recognized and recorded, and the

problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate penetration testing into our audits of information security. Such tests involve attempting, with agency cooperation, to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. As we reported in 1998, our auditors have been successful, in almost every test, in readily gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purpose they had in mind.

Application Software Development and Change Controls

Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and to ensure that different versions are not misidentified.

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

Weaknesses in software program change controls were identified for 19 of the 21 agencies where such controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. At another, documentation was not retained to demonstrate user testing and acceptance.

-
- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of “locally developed” unauthorized software programs was prevented or detected.
 - Agencies’ policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

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

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

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

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a combination of physical and logical access controls and by effective supervisory review.

Segregation of duties was evaluated at 20 of the 24 agencies covered by our analysis, and weaknesses were identified at 17 of these agencies. Common problems involved computer programmers and operators who were authorized to perform a wide variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security

features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duty problems also were identified related to transaction processing. For example, at one agency, 11 staff involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 staff had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about \$300,000, that were requested, approved, and receipt recorded by the same individual.

System Software Controls

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

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

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier in this section. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them.

Operating system software controls were covered in audits for 18 of the 24 agencies included in our review. This was a significant increase over 1998, when we reported that this important control area had been reviewed for only 9 agencies.

Weaknesses were identified at each of the 18 agencies for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a wide variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Service Continuity Controls

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

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

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. If controls are inadequate, even relatively minor

interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity controls were evaluated for 21 of the 24 of the agencies included in our analysis. Of these 21, weaknesses were reported for 20 agencies. Examples of weaknesses included the following:

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

Conclusions

The expanded body of audit evidence that has become available since we reported on the status of federal information security in September 1998 shows that important operations at every major federal agency continue to be at risk as a result of weak information security controls. There are many specific causes of these weaknesses, but an underlying problem is poor security program management and poor administration of available control techniques. While agencies have taken steps to address problems and many have remedial efforts underway, audits completed over the past year show that agencies have not implemented fundamental management practices needed to ensure that their computer-based controls remain effective on an ongoing basis.

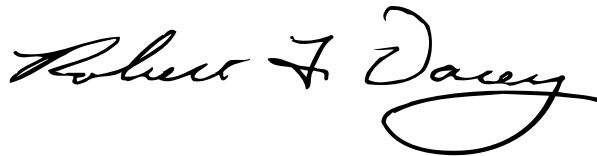
The audit reports cited in this report include many recommendations to individual agencies that address the specific weaknesses reported. For this reason, we are making no additional recommendations to these agencies in this report. However, we have issued two executive guides that discuss practices that leading organizations have employed to strengthen the effectiveness of their security programs. These executive guides are

Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998) and *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33, November 1999).

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies to The Honorable Jacob Lew, Director of the Office of Management and Budget, and the Heads, Chief Information Officers, and Inspectors General of the 24 federal departments and agencies covered by our review. We are also sending copies to the Chairs and Ranking Minority Members of the Senate Governmental Affairs Committee and the House Committee on Government Reform, as well as to other interested members of the Congress. Copies will be made available to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-3317 or by e-mail at dacey.aimd@gao.gov.

Sincerely yours,

A handwritten signature in black ink, reading "Robert F. Dacey". The signature is fluid and cursive, with the first name "Robert" and last name "Dacey" clearly legible. The middle initial "F." is written in a smaller, more compact script.

Robert F. Dacey
Director
Information Security Issues

Objectives, Scope, and Methodology

Our objectives were to (1) analyze and summarize information security weaknesses identified in audit reports issued from July 1999 through August 2000 and compare these findings with similar information that we reported in September 1998, (2) identify examples of weaknesses and the related risks at selected individual agencies, and (3) identify the most significant types of weaknesses in each of six categories of general controls that we used in our analysis.

We analyzed findings from over 50 GAO and agency reports, including inspector general reports, issued from July 1999 through August 2000. The reports we considered pertained to the 24 federal departments and agencies covered by the Chief Financial Officers Act. Together these departments and agencies accounted for about 99 percent of the total reported federal net outlays in fiscal year 1999.

In analyzing reported findings, we categorized them into six basic areas of general control: security program planning and management, access control, application program change control, segregation of duties, operating systems security, and service continuity. These six areas of general controls provide a framework for comprehensively evaluating information security that is described in GAO's *Federal Information Systems Controls Audit Manual*.

Our analysis was performed during August 2000 in accordance with generally accepted government auditing standards.

GAO Contacts and Staff Acknowledgments

GAO Contact

Jean Boltz, (202) 512-5247, boltzj.aimd@gao.gov

Acknowledgments

Other major contributors to this work were Debra Conner, John de Ferrari, David Irvin, Elizabeth Johnston, Sharon Kittrell, Jeffrey Knott, Carol Langelier, Colleen Phillips, Alicia Sommers, Crawford L. Thompson, William Thompson, and Gregory Wilshusen.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

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

Orders by visiting:

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

Orders by phone:

(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

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

Orders by Internet:

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>

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

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

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

Bulk Rate Postage & Fees Paid GAO Permit No. GI00

