GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-284007

November 10, 1999

The Honorable Dianne Feinstein
Ranking Minority Member
Subcommittee on Technology, Terrorism
and Government Information
Committee on the Judiciary
United States Senate

Subject: Information Security: Weaknesses at 22 Agencies

Dear Senator Feinstein:

On October 6, 1999, I testified before the Subcommittee on the need for improved federal information security.[1] I noted that audits by GAO and agency inspectors general show that 22 of the largest federal agencies were not adequately protecting critical federal operations and assets from computer-based attacks. I concluded that addressing this widespread and persistent problem would require significant management attention and action within individual agencies as well as increased coordination and oversight at the governmentwide level.

During the question-and-answer period of that hearing, you requested that we provide summaries of significant information security weaknesses previously reported at those 22 federal agencies. My response to your request is included in the two enclosures to this letter.

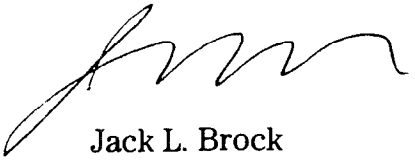
Enclosure 1 provides brief summaries of the reported information security weaknesses at each of the 22 federal agencies and cites the reports from which this information was drawn. These reports were issued from May 1998 through October 1999, and they describe conditions that existed at the time of the related audits. Since then, many agencies have undertaken efforts to correct reported weaknesses. However, until the results of subsequent audits become available, we cannot assess the effectiveness of these corrective actions.

[1]Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations (GAO/T-AIMD-00-7, October 6, 1999).

Enclosure 2 lists GAO reports that chronicle our assessments of federal information security since 1993. These reports provide additional insight into widespread information security weaknesses in the federal government.

We are sending a copy of this response to the Honorable John Kyl, Chairman, Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary. Please contact me at (202) 512-6240 or Bob Dacey, Director, Consolidated Audit and Computer Security Issues, at (202) 512-3317, if your or your staff have any questions. I can also be reached by e-mail at *brockj.aimd@gao.gov*. Key contributors to this summary were Jean Boltz, David Irvin, and Jeffrey Knott.

Sincerely yours,



Jack L. Brock
Director, Governmentwide and Defense
Information Systems

Enclosures

Information Security Weaknesses Reported for Federal Agencies From May 18, 1998 to October 4, 1999

Department of Agriculture

In July 1999, we reported that the Department of Agriculture's (USDA) National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent and/or detect unauthorized changes to payroll and other payment data or computer software. NFC develops and operates administrative and financial systems, including payroll/personnel, property management, and accounting systems for both the USDA and over 60 other federal organizations. During fiscal year 1998, NFC processed more than $19 billion in payroll payments for more than 450,000 federal employees. NFC is also responsible for maintaining records for the world's largest 401(k)-type program, the federal Thrift Savings Program. This program, which is growing at about $1 billion per month, covers about 2.3 million employees and had over $60 billion in assets as of September 30, 1998. The weaknesses we identified increased the risk that users could cause improper payments and that sensitive information could be misused, improperly disclosed, or destroyed. Also, in February 1999, the USDA IG reported that Rural Development had not implemented a "firewall system" to provide security over Internet telecommunications.

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-99-227, July 30, 1999) and U.S. Department of Agriculture Consolidated Financial Statements for Fiscal Year 1998, Audit Report No. 50401-30-FM, February 1999.

Department of Commerce

In March 1999, the Department of Commerce Inspector General (IG) reported weaknesses in the Department's information system controls. The review found that formal, comprehensive security policies did not exist or were incomplete. Also, controls over access to operating systems and the associated financial applications were inadequate, and controls associated with the procedures for making software changes were weak. Weaknesses also existed in properly segregating duties and controlling physical access to the data centers. Furthermore, disaster recovery plans were incomplete or outdated.

U. S. Department of Commerce Fiscal Year 1998 Consolidated Financial Statements, Office of Inspector General, Audit Report No. FSD-10899-9-0001, March 1999.

Department of Defense

In August 1999, we reported that serious weaknesses in Department of Defense (DOD) information security continue to provide both hackers and hundreds of

thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data. These weaknesses impair 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 Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks or fraud.

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

Department of Education

In May 1998, the Department of Education IG reported that improvements were required in security over financial systems and in disaster recovery capabilities. The deficiencies in the department's payment system could have enabled unauthorized users to access confidential data, change data, make unauthorized payments, or bring down the system. The payment system was used to annually process about $33 billion in grant and contract disbursements. Education decided to spend minimal resources on the system, which was replaced in fiscal year 1998 with a core financial management system.

Annual Accountability Report – Fiscal Year Ended September 30, 1997, Office of the Chief Financial Officer, July 21, 1998. (As of October 15, 1999, the Department of Education IG had not published its fiscal year 1998 consolidated financial statement audit report, which is expected to include an updated assessment of information system general controls.)

Department of Energy

In its fiscal year 1998 accountability report, the Department of Energy (DOE) recognized the need to improve unclassified computer security, noting the apparent increase in system and network vulnerabilities at the department. Such vulnerabilities increase the likelihood of unauthorized intrusions into DOE's publicly available systems. The report states that one of the primary causes was the lack of a meaningful policy and program framework, while another root cause was the lack of awareness of system vulnerabilities by employees, line managers, and upper management.

U.S. Department of Energy Fiscal Year 1998 Accountability Report, DOE/CR-0067, February 1999.

Environmental Protection Agency

In September 1999, the Environmental Protection Agency (EPA) IG reported weaknesses in critical mainframe operating system software controls. These weaknesses could affect system integrity, or allow a knowledgeable user to circumvent or disable security mechanisms and/or modify programs or data files on the computer without leaving an audit trail. The IG also identified continuing security concerns for regional computer facilities and data, citing weaknesses in security planning, contingency and disaster recovery planning, and security training.

Environmental Protection Agency Office of Inspector General Audit Report - Financial Management: Audit of EPA's Fiscal 1998 Financial Statements, Report Number 99B0003, September 28, 1999.

Federal Emergency Management Agency

In February 1999, as part of its audit of the Federal Emergency Management Agency's (FEMA) financial statements, an independent accounting firm reported information system security and access control deficiencies. The firm concluded that these deficiencies indicate that FEMA's computer-based controls do not contribute to the reliability of the accounting systems.

Federal Emergency Management Agency Office of Inspector General Audit Division, Auditor's Report on FEMA's Fiscal Year 1998 Financial Statements, H-6-99, March 1999.

General Services Administration

In February 1999, an independent accounting firm recommended that GSA (1) strengthen logical and physical access controls over its information technology environment, and (2) apply security policies and procedures uniformly across service lines. The firm's review of four GSA systems identified weaknesses associated with (1) logical access granted being consistent with job responsibilities, (2) controls to monitor and detect unauthorized access, (3) physical access to computer resources, and (4) access privileges for users who had been terminated or had changed job responsibilities. These four systems include processes for accounting, tracking real property, supporting GSA's worldwide supply function, and managing its motor vehicle fleet. The firm also found that security policies and procedures throughout GSA did not in all cases address control issues such as password administration and management, access violation monitoring, and security awareness training. In the absence of certain preventive and detective controls, GSA cannot ensure that its mission critical applications and data are protected from unauthorized access, modification, or deletion by internal users or external sources.

GSA 1998 Annual Report, February 1999.

Department of Health and Human Services

In February 1999, the Health and Human Services IG reported serious control weaknesses associated with the Department's Health Care Financing Administration (HCFA) computers. HCFA relies on extensive automated operations at both its central office and the Medicare contractors to administer the Medicare program and to process and account for Medicare expenditures. The HCFA central office maintains administrative data, such as Medicare enrollment, eligibility, and paid claims data, and processes all payments for managed care. In fiscal year 1998, managed care payments totaled $33 billion.

United States Department of Health and Human Services, Accountability Report: Fiscal Year 1998, February 26, 1999.

Department of Housing and Urban Development

In March 1999, the Housing and Urban Development (HUD) IG reported the need for improvements related to general system security, administration of personnel security operations, and access controls over HUD's two major payment systems. The IG identified general system security weaknesses associated with protecting sensitive and critical mainframe systems, administering local area network passwords, monitoring network security, developing and testing disaster recovery plans, and controlling software changes for critical mainframe applications. HUD's automated information systems are critical in supporting all facets of its programs, including mortgage insurance, servicing, and administrative operations. During fiscal year 1998, HUD's two major payment systems processed disbursements for approximately $33 billion, including support of Section 8 programs and a broad range of grants to states, municipalities, independent companies, nonprofit institutions, and individuals.

Office of Inspector General Audit Report - US Department of Housing and Urban Development Audit of Fiscal Year 1998 Financial Statements, 99-FO-177-0003, March 29, 1999.

Department of the Interior

In April 1999, the Interior IG reported general control weaknesses at the Bureau of Indian Affairs and the U.S. Geological Survey. The IG considered general controls over certain automated information systems operated by the Bureau of Indian Affairs to be ineffective. For example, the Bureau did not (1) have an effective security program, (2) classify resources to determine the security level needed, (3) properly safeguard computer hardware, (4) perform reviews to ensure

appropriate user access levels, (5) have segregation of duties for system support functions, (6) have controls over system software to effectively detect and deter inappropriate use, and (7) have an effective means of recovering or continuing computer operations in the event of system failure. The IG also reported that security weaknesses identified at one of the U.S. Geological Survey's data centers increased the risk of unauthorized access and modifications to, and disclosure of, information processed on the data center's mainframe computer.

Fiscal Year 1998 Interior Accountability Report, April 1999.

Department of Justice

In February 1999, the Department of Justice IG reported that improvements were needed in general controls at the department's data centers and component financial management systems. For example, at the Federal Bureau of Investigation, improvements were needed to correct deficiencies associated with entitywide security program enhancements, logical access controls, a formal change control process, and a comprehensive, tested business continuity plan. The Drug Enforcement Administration lacked an incident response training program for certain systems, a disaster recovery plan that includes alternate backup sites, and access controls that ensure transferred or terminated employees are promptly removed from user access files. Similar issues were noted at the Immigration and Naturalization Service and the U.S. Marshals Service. The control weaknesses identified increase the risk that software programs and data processed on these systems are not adequately protected from unauthorized access.

U. S. Department of Justice Annual Financial Statement Fiscal Year 1998, Office of the Inspector General, Report Number 99-05, February 1999.

Department of Labor

In February 1999, the Department of Labor IG reported weaknesses associated with entitywide security, access controls, and application software development and change control. For example, standard security-related personnel policies had not been developed or coordinated for five of the six systems reviewed. As a result, these systems were exposed to potential risks that may result from accidental and/or intentional personnel security failures or violations. Also, for five of the six systems reviewed, independent risk assessments had not been performed or properly documented on a regular basis or whenever systems had changed. If risk assessments are not performed, then it is likely that threats and vulnerabilities are not being identified and considered.

U. S. Department of Labor Consolidated Financial Statement Audit, Office of Inspector General, Report Number 12-99-002-13-001, February 26, 1999.

National Aeronautics and Space Administration

In May 1999, we reported that, as part of our tests of the National Aeronautics and Space Administration's (NASA) computer-based controls, we successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for earth orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. Having obtained access, we could have disrupted ongoing command and control operations and stolen, modified, or destroyed system software and data. A major factor in our ability to penetrate these systems was that NASA was not effectively managing information security throughout the agency.

Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD-99-47, May 20, 1999).

Office of Personnel Management

In February 1999, an independent accounting firm reported weaknesses in OPM's entity-wide security program, access controls, application change control, and service continuity based on its overall assessment of OPM's information system control environment. The firm found that the Retirement and Insurance Service's mainframe security policies did not specifically address important aspects of security, and its local area network did not have formal documented security policies and procedures. As a result, security controls may be inadequate, responsibilities may be unclear, and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

Office of Personnel Management – Financial Statements - Retirement Program, Health Benefits Program, Life Insurance Program - Fiscal Year 1998, Report Number 2F-00-98-103, March 1, 1999.

Small Business Administration

In September 1999, the Small Business Administration (SBA) IG reported that SBA's general controls did not fully comply with established policies and procedures. For example, (1) SBA had not funded and implemented an entitywide security program, (2) unnecessary and excessive access privileges reduced accountability and created segregation of duties weaknesses, (3) application development and change control procedures were not consistently applied in systems outside the Office of the Chief Information Officer's control, (4) programmers' abilities to access operating systems could not be monitored, and (5) security administrators and program managers needed training. As a result of such weaknesses, SBA personnel, contractors, and business partners had access to information and functions involving loan applications, financial

obligations, collections, disbursements, and write-offs that may be unnecessary or reduce accountability. This increased the risks of financial loss and misuse of information.

Audit of SBA's Information Systems Controls, U.S. Small Business Administration, Office of Inspector General, Audit Report Number 9-19, September 2, 1999.

Social Security Administration

In November 1998, an independent accounting firm found that the Social Security Administration's (SSA) systems environment remained threatened by weaknesses in several components of its information protection control structure. Weaknesses were noted in the entitywide security program, and associated weaknesses were identified in local area network and distributed systems security, SSA's mainframe computer security (controlling access to sensitive information), and physical access controls. The firm concluded that, until corrected, these weaknesses would continue to increase the risks of unauthorized access to, and modification or disclosure of, sensitive SSA information. In turn, unauthorized access to sensitive data can result in the loss of data, loss of trust fund resources, and compromised privacy of information associated with SSA's enumeration, earnings, retirement, and disability processes and programs. SSA programs disbursed about $416 billion in fiscal year 1998, and delivered cash benefits to about 50 million beneficiaries every month.

Social Security Administration Accountability Report for Fiscal Year 1998, November 20, 1998.

Department of State

In August 1999, an independent accounting firm reported that the Department of State's mainframe computers for domestic operations are considered vulnerable to unauthorized access. Consequently, other systems, which process data using these computers, may also be vulnerable. Similar weaknesses were found in the Paris Financial Service Center's Accounting and Disbursing Center. A year earlier, in May 1998, we had reported that our tests at State demonstrated that its computer systems and the information they maintained were very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses. For example, without any passwords or specific knowledge of State's systems, we successfully gained access to State's networks through dial-in connections to modems. Having obtained this access, we could havemodified, stolen, downloaded, or deleted important data; shut down services; and monitored network traffic, such as e-mail and data files. In addition, we were able to circumvent State's internal network security controls and access information and sensitive data that would normally be off limits to most employees.

Audit of the Department of State's 1997 and 1998 Principal Financial Statements, Leonard G. Birnbaum and Company, LLP, August 9, 1999; Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998).

Department of Transportation

In March 1999, the Department of Transportation IG reported that DOT's Intermodal Data Network, which connects local area networks within DOT agencies, was found vulnerable to unauthorized access. This weakness was identified in fiscal year 1996 and considered on target for correction as of December 1998. DOT was continuing work to ensure that weaknesses identified in a previous GAO report were corrected. In May 1998, we reported that the Federal Aviation Administration's controls were ineffective in all critical areas included in our security review, including facilities physical security, operational systems information security, future systems modernization security, management structure, and policy implementation. Vulnerabilities created by inadequate controls place the safety of the airplane passengers at risk, while sensitive information could be compromised and flight services interrupted.

Office of Inspector General Audit Report - Fiscal Year 1998 Consolidated Financial Statements, Department of Transportation, Report Number FE-1999-081, March 30, 1999, and Air Traffic Control: Weak Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

Department of the Treasury

In December 1998, we reported that weaknesses in the Internal Revenue Service's (IRS) computer security controls continued to place IRS' automated systems and taxpayer data at serious risk to both internal and external threats that could result in the denial of computer services or in the unauthorized disclosure, modification, or destruction of taxpayer data. Also, in October 1999, we reported that general computer controls at the Department's Financial Management Service and its contractor data centers placed its financial systems at significant risk of unauthorized disclosure and modification of sensitive data and programs, misuse or damage to computer resources, or disruption of critical operations. As a result, billions of dollars of payments and collections were at risk of fraud.

IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk (GAO/AIMD-99-38, December 14, 1998) and Financial Management Service: Significant Weaknesses in Computer Controls (GAO/AIMD-00-4, October 4, 1999).

Department of Veterans Affairs

In October 1999, we reported that Department of Veterans Affairs (VA) systems continued to be vulnerable to unauthorized access. VA operates the largest health

care delivery system in the United States and reported spending more than $17 billion on medical care in fiscal year 1998. The department also processed more than 42 million benefit payments totaling about $22 billion in fiscal year 1998 and provided life insurance protection through more than 2.4 million policies that represented about $23 billion in coverage. In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for veterans and their family members. We, as well as the VA IG, continued to find serious problems that placed sensitive information at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. For example, at one VA insurance center, 265 users who had not been authorized to perform data entry had the ability to read, write, and delete information related to insurance awards. Such unauthorized access could lead to improper insurance payments.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs (GAO/AIMD-00-05, October 4, 1999).

U.S. Agency for International Development

In March 1999, the U. S. Agency for International Development (USAID) IG reported that USAID's client-server and mainframe general controls are not effective. Specifically, the audit found that USAID's (1) entitywide security program and management, (2) access controls, (3) application software development and change control, and (4) segregation of computer system duties provided inadequate control over client-server and mainframe operations. Also, deficiencies were noted for system software controls and continuity of services for the client-server computer environment. Because of these weaknesses, USAID lacks the assurance that the data are accurately processed or that systems and data are adequately secured. A primary reason for the ineffective controls is the lack of an agencywide security program that includes clear security responsibilities and agencywide security processes.

Audit of General Controls Over USAID's Mainframe Computer Environment, Office of the Inspector General, Audit Report No. A-000-99-004-P, March 1, 1999 and Audit of General Controls Over USAID's Client-Server Computer Environment, Office of the Inspector General, Audit Report No. A-000-99-005-P, March 1, 1999.

GAO Information Security Reports and Testimony Issued Since September 1993

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations (GAO/T-AIMD-00-7, October 6, 1999).

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

Information Systems: The Status of Computer Security at the Department of Veterans Affairs (GAO/AIMD-00-5, October 4, 1999).

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences (GAO/AIMD-00-1, October 1, 1999).

Information Security: The Proposed Computer Security Enhancement Act of 1999 (GAO/T-AIMD-99-302, September 30, 1999).

Federal Reserve Banks: Areas for Improvement in Computer Controls (GAO/ AIMD-99-280, September 15).

Information Security: NRC's Computer Intrusion Detection Capabilities (GAO/ AIMD-99-273R, August 27, 1999).

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

Battlefield Automation: Opportunities to Improve the Army's Information Protection Effort
(GAO/NSIAD-99-166, August 11, 1999).

Information Security: Answers to Posthearing Questions(GAO/AIMD-99-272R, August 9, 1999).

Bureau of the Public Debt: Areas for Improvement in Computer Controls (GAO/ AIMD-99-242, August 6, 1999).

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

Medicare: Improvements Needed to Enhance Protection of Confidential Health Information (GAO/HEHS-99-140, July 20, 1999).

Medicare: HCFA Needs to Better Protect Beneficiaries' Confidential Health Information (GAO/T-HEHS-99-172, July 20, 1999).

Information Security: Recent Attacks on Federal Web Sites Underscore Need for Strengthened Information Security Management (GAO/T-AIMD-99-223, June 24, 1999).

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls (GAO/AIMD-99-161, June 8, 1999).

Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD-99-47, May 20, 1999).

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).

Financial Audit: 1998 Consolidated Financial Statements of the United States Government (GAO/AIMD-99-130, March 31, 1999).

Securities Fraud: The Internet Poses Challenges to Regulators and Investors (GAO/T-GGD-99-34, March 22, 1999).

IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk (GAO/AIMD-99-38, December 14, 1998).

Financial Management Service: Areas for Improvement in Computer Controls (GAO/AIMD-99-10, October 20, 1998).

Federal Reserve Banks: Areas for Improvement in Computer Controls (GAO/AIMD-99-6, October 14, 1998).

Bureau of the Public Debt: Areas for Improvement in Computer Controls (GAO/AIMD-99-2, October 14, 1998).

Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

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

Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets (GAO/T-AIMD-98-312, September 23, 1998).

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

Defense Information Superiority: Progress Made, but Significant Challenges Remain (GAO/NSIAD/AIMD-98-257, August 31, 1998).

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

DOD's Information Assurance Efforts (GAO/NSIAD-98-132R, June 11, 1998).

Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk (GAO/T-AIMD-98-170, May 19, 1998).

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

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

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

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

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

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

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

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

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

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

Budget Process: Comments on S.261–Biennial Budgeting and Appropriations Act (GAO/T-AIMD-97-84).

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

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

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

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

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

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

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

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

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

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

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

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

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1994 and 1995 (GAO/AIMD-96-22, February 26, 1996).

Financial Management: General Computer Controls at the Senate Computer Center (GAO/AIMD-96-15, December 22, 1995).

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).

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 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).

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

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

(511863)

Ordering Information

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

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

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

http://www.gao.gov

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

Bulk Mail
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested