122613
~~26514~~

U. S. GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 A.M., EST
MONDAY, OCTOBER 17, 1983

STATEMENT OF

WARREN G. REED

DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
COMMITTEE ON SCIENCE & TECHNOLOGY

HOUSE OF REPRESENTATIVES

ON

TELECOMMUNICATIONS SECURITY AND PRIVACY

122613
026927

Mr. Chairman and Members of the Subcommittee:

We are here today at your request to discuss telecommunications and related computer security and privacy issues. Our testimony is based on the knowledge of the subject we gained in numerous audits of federal government executive departments and agencies over the past several years.

In this testimony I will discuss the information security environment from four different standpoints. First, I will discuss the nature of the information security problem today as it affects our automated systems and, increasingly, their supporting telecommunications networks. I will describe the different types of threats we must protect our systems against and indicate the reasons why the problem is growing more serious. Second, I will describe the key factors of legislation, policy, management, and auditing which affect information security. Third, I will summarize our audit findings over the past 7 years in relation to these key factors and indicate shortfalls which have contributed to security problems. Finally, I will discuss recent federal initiatives that, collectively, could have an important impact on solving these problems.

Our basic message is that the vulnerabilities facing our computer systems and telecommunications networks are increasing as technology advances. The growing numbers of remote computer terminals which provide access to very large data bases make errors or deliberate attacks difficult to discover and fix. Legislation, policies, management roles, and audits provide a framework for counteracting these vulnerabilities but further steps are needed. In particular, agencies need to devote more management attention and resources to implementing total systems of control. Government-wide and agency-specific activities underway appear to be fostering this goal.

THE NATURE OF THE INFORMATION SECURITY PROBLEM

The federal government depends heavily on computers and telecommunications networks today to handle information on functions ranging from defense and intelligence to banking and financial activities, health, and education. Much of this information is personal, proprietary, or otherwise sensitive and requires effective security. Information security has three basic components: computer security, telecommunications security, and supporting systems security.

GAO reports since 1976 and examinations by others have repeatedly demonstrated that federal information systems are subject to three broad categories of threat: (a) natural hazards,

(b) unintentional actions, and (c) intentional actions. Natural hazards include fire, floods, earthquakes, etc., that can damage or totally destroy equipment, software, and data or seriously interrup operations through extended power outages. Unintentional actions include equipment failures and malfunctions and improper design of systems failures as well as personnel errors and inappropriate actions. The latter two pose the more serious threats. Intentional actions, which receive considerable attention, include attacks on equipment, improper access to and disclosure of information which should be held private, and unauthorized alteration of official records. A variety of technical methods can be used to penetrate computer systems for these purposes.

Providing a reasonable level of protection in today's technological environment is a formidable challenge because the range of vulnerabilities is increasing. The larger systems in use can store more sensitive information in electronic form. The expanded use of remote terminals provides more isolated points of access and makes it difficult to pinpoint errors or attacks. Similarly, the advent of microcomputers provides more individuals with the potential capability to access, create, and manipulate

data bases by bypassing central controls. The trend toward linking computers and terminals through telecommunications networks provides potential penetrators with more opportunities, techniques, and devices to access systems, to insert communications, and to intercept and interpret communications.

In spite of the sophistication and complexities of our hardware, software, and communications networks, we must keep in mind that information security is basically a management problem, not a technology problem, and requires a concerted management solution.

KEY FACTORS AFFECTING INFORMATION SECURITY

Legislation, policy, management by central and executive agencies, and auditing are the key factors that support Federal efforts to provide security.

Legislation

Legislation serves to define information security goals and objectives and to assign overall management responsibilities for security. A variety of laws have been enacted governing different security activities.

The Brooks Act of 1965 (Public Law 89-306), which amended the Federal Property and Administrative Services Act of 1949, assigned the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Department of Commerce collective responsibility for managing agencies' acquisition and maintenance of ADP resources, but placed OMB in a leadership role. The Federal Communications Act of 1934, as later modified by the Omnibus Crime Control and Safe Streets Act of 1968 (Public Law 90-351), provided for the protection of electronic transmissions. The Privacy Act of 1974 (Public Law 93-579) prescribed controls over personal records dissemination and access. The Paperwork Reduction Act of 1980 (Public Law 96-511) broadened OMB's responsibilities in the context of information resources management. Finally, the Federal Managers' Financial Integrity Act of 1982 (Public Law 97-255) directed evaluations of administrative and financial internal control systems and agency accounting systems. It further required annual reports on these systems. In 1983 GAO published standards for Internal Controls in the federal government to be used by agencies to establish and maintain effective systems of internal control in compliance with the act.

Policy

Information security policy should provide agencies with a clear and concise blueprint for implementation of relevant

legislation. It should faithfully reflect legislative intent, completely address all pertinent features of the legislation, and be compatible with other related policies.

OMB is the key policymaker in this area. Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Systems," issued July 27, 1978, outlines basic policy and specifies agencies' responsibilities for the development and implementation of security. In particular it assigns government-wide responsibilities to GSA, Commerce, and the Office of Personnel Management (OPM). OMB Circular A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," issued July 1, 1975, requires agencies to establish reasonable safeguards against improper disclosure of such records. OMB Circular A-123, "Internal Control Systems," revised August 16, 1983, after passage of the Financial Integrity Act, prescribes policies and guidance for establishing and maintaining internal controls over program and administrative activities. It mandates that all levels of agency management help assure the adequacy of these controls.

Management

Management responsibilities are divided among four "central agencies" (OMB, GSA, Commerce, and OPM) and the remaining executive agencies.

The central agencies should issue policies, guidelines, and regulations that are consistent and coordinated with each other and contain "how-to" specifics where applicable to assist executive agencies in meeting legislative and Executive Office requirements. They also should oversee agencies' implementation of their guidance.

The central agencies have related yet separate responsibilities. OMB must review agencies' organizational structures and management procedures to ensure they meet policy requirements. GSA is required to issue policies and regulations for the physical security of computer rooms and to ensure that agency procurement requests for computers include appropriate security requirements. The Department of Commerce is responsible for developing uniform federal ADP standards including security standards. It has delegated this responsibility to the National Bureau of Standards (NBS). OPM is responsible for establishing personnel security policies for federal personnel associated with the design, operation, or maintenance of computer systems or having access to data in these systems.

The executive agencies play the most vital role in protecting our information assets. They must develop and implement agency information security programs through a set of policies and procedures which conform to the requirements of applicable legislation and guidance. Their security programs should provide a reasonable, yet cost-effective, level of protection. Agency

management should base their programs on assessments of risk and ensure that they incorporate administrative, physical, as well as technical controls. Finally, agency management must monitor the implementation of their programs.

Agency managers employ a wide variety of techniques to achieve a total system of control. A technique known as risk analysis is used to ascertain the extent to which information systems are vulnerable to natural disaster, human error, and improper or illegal use. This provides a basis for a program to minimize the effects of such vulnerability. Other related techniques include background investigations for employees and contractors associated with computers; contingency plans for emergency response in the event of system failure; backup and recovery capabilities to keep systems operating in the wake of disaster; and the use of encryption devices to protect personal data transmissions.

Audits

Systematic internal audits provide management with periodic reports on the level of protection actually provided over automated systems and particularly their sensitive applications. Management can use these reports to identify needed corrective measures.

OMB Circular A-71, Transmittal Memorandum No. 1, requires agencies to conduct periodic audits of security safeguards. It specifies that these audits be performed by an organization independent of the user organization and computer facility managers.

The Comptroller General has issued specific standards for auditing programs supported by computer-based systems. These standards prescribe that auditors review both general systems and applications controls. They also suggest that reviews be conducted during the early stages of system design and development. Circular A-123 requires that agencies provide for ongoing internal control reviews and that agency inspectors general assist in this process.

GAO AUDIT FINDINGS RELATED TO KEY FACTORS

Since April 1976 GAO has issued about 40 reports related to information security. These reports have identified deficiencies in several areas including the following (numbers are approximate):

--Legislation (1).

--Policy (10).

--Management (15).

Central agency and executive agency management (7).

Internal controls (8).

--Internal audit (3).

Many issues have been reported on repeatedly during this period. For example, the first GAO report on the implementation of Circular A-71, Transmittal Memorandum No. 1, was issued in 1979 and at least six other reports addressed this issue in 1979, 1980, 1982, and 1983. We have not comprehensively updated our major security findings since 1982; however, we have performed work at selected agencies. I will highlight our findings bearing directly on information security.

Legislation

Our review of applicable telecommunications security legislation showed that the Communications Act of 1934 and the Crime Control Act of 1968 are inadequate with respect to interceptions of wire communications, or "wiretapping." The 1934 Communications Act did not define the term "interception." The Crime Control Act of 1968, as amended, used the qualifying term "aural acquisition" (acquired by use of the ear) to define interception. As a result, only interceptions by aural means are illegal under

this act, unless authorized by court order. Therefore, we conclude that as long as the term "aural" remains as a semantic qualifier in the 1968 Crime Control Act's definition of interception, anyone can conduct unauthorized nonaural wiretapping of data telecommunications without a court order and not be in violation of this law.

The definition of interception under the Crime Control Act of 1968 is conceptually different from the definition of "electronic surveillance" in the Foreign Intelligence Surveillance Act of 1978, Section 1801 of Title 50, United States Code, which by definition is not limited to "aural" interception.

Policy

We reported that OMB Circular A-71, Transmittal Memorandum No. 1, the primary Federal guidance for information security, needed revision, in part, to:

--Identify the minimum controls necessary to ensure a reasonable level of protection over personal, proprietary, and other sensitive information.
--Clarify when executive agencies must afford the same level of protection for such sensitive information as they do for information classified for purposes of national security.

--Establish policy and specific guidance for protecting systems using telecommunications networks.

Management

We have reported that the central agencies had provided incomplete and uncoordinated guidance and had not ensured that agencies complied with existing guidance.

OMB issued pertinent circulars such as Circular A-71, Transmittal Memorandum No. 1, and Circular A-123 on internal controls. However, it had not taken adequate action to ensure that executive agencies were effectively implementing their information security programs in compliance with Circular A-71, Transmittal Memorandum No. 1 which we stated should be revised.

GSA had not adequately cross-referenced the Federal Property Management Regulations (FPMRs) on ADP and telecommunications with the applicable NBS Federal Information Processing Standards Publications (FIPS PUBS) on security.

NBS planned to issue 36 standards it considered necessary to achieve a reasonable level of protection over executive agencies' automated information systems. However, we reported in 1982 that NBS had issued only six guidelines and one standard addressing various aspects of security.

OPM's guidance for personnel security needed strengthening. For example, the "grandfather" provision in OPM's Federal Personnel Management Letter 732-7 permitted many experienced employees to receive security approvals without a background investigation appropriate to the sensitivity of their positions.

Regarding executive agency management, we reported that the executive agencies were doing little to implement information security program policies and guidance. Further, we reported that some senior managers were not fully aware of how highly vulnerable their systems are to fraudulent, wasteful, abusive, and illegal practices. For example, in September 1983 we reported that the Arms Control and Disarmament Agency had not developed an information security program, had not performed required risk analyses, and had not conducted required security audits. As a result, management could not be sure computerized information was adequately protected. A key computer services official believed the potential existed for loss of valuable data.

We found that most executive agencies generally selected, implemented, and maintained a system of controls based on personal insight rather than on the use of risk analysis techniques. Risk analysis techniques provide a sound basis for management to implement and maintain a total system of controls which balances the

costs of protection against the risks posed by fraudulent, wasteful, abusive, and illegal activities and natural disasters. The most cost-effective time to incorporate such controls into a system is when it is being designed.

Required personnel background investigations were not always performed. For example, we reported that the security officers at two agencies did not have extensive background investigations completed for themselves, even though both occupied positions defined by OPM as being highly sensitive. The omissions occurred because the agencies that employed them had not defined their positions in accordance with OPM guidance.

Audits

We reported at least three major areas in which Federal internal audit units had not met their automated information system responsibilities.

First, we found that several internal audit organizations had not provided adequate audit coverage for their agencies' computer systems and applications. One reason was that, although Circular A-71, Transmittal Memorandum No. 1, required such audits, it did not specifically assign them to the internal audit function.

Second, we reported that internal auditors did not always comply with Comptroller General audit standards for reviewing computer-based systems.

Third, we reported that many audit organizations had not developed or maintained appropriately skilled audit staff. Staffing was hindered by lack of management support, personnel ceilings, and hiring restrictions. We identified the need for formal training programs for automated information system auditing.

We believe this synopsis of GAO's audit findings of the past few years provides ample evidence that serious shortfalls exist in each factor relating to information security. We have found policy gaps, serious management deficiencies at both the central and executive agency level, inadequate internal audit capabilities, and at least one needed revision to law. Because of these shortfalls, information system losses continue to occur due to accidental and intentional causes. For example, we reported that in April 1982 the U.S. Attorney's Office in Los Angeles successfully prosecuted a Social Security Administration field office employee who had fraudulently used the telecommunications network to steal more than $104,000 in supplemental security income benefits. This was the third such case prosecuted by that office since 1980. We also reported that in 1981 the military services

overpaid military retirees and survivors about $5 million because the Veterans Administration did not inform the services that it had paid compensation to these individuals. The Veterans Administration's failure to inform the services through its automated information system was due to a combination of (1) clericial oversight or error in not reporting award data and (2) incomplete records that did not indicate the award recipient was a military retiree or survivor.

CURRENT ACTIVITIES TO IMPROVE SECURITY

To place the above findings in perspective, we have attempted to identify current initiatives in each of the four categories of supporting factors that may become vehicles for enhancing security.

Legislation

Proposed legislation addresses computer crime

Identical bills were introduced in the House and Senate this year which would establish criminal penalties for fraudulent or illegal use of computers owned by, operated by, or under contract to the U.S. Government. H.R. 1092 and S. 1733, "The Federal Computer Systems Protection Act," stem from the recognition that,

although computer or information system crimes can cause substantial financial loss, they have been difficult to prosecute under existing laws. If passed, the legislation could potentially help the government take punitive action against those who intentionally misuse its automated systems.

Policy

OMB plans to revise existing circulars on information management

In a September 12, 1983, Federal Register notice, OMB announced plans to develop a new policy circular on federal information management. The proposed circular would consolidate four existing circulars, including Circular A-71, Transmittal Memorandum No. 1, on information security and Circular A-108 on the maintenance of records about individuals. OMB is considering framing the circular to address a wide range of issues which go beyond the scope of current policy. One such issue is the security implications of the new environment of end user computing, which can involve telecommunications networks and microcomputers.

Thus, although OMB did not respond to our April 1982 recommendation that it revise Circular A-71, Transmittal Memorandum No. 1, its plans for a comprehensive information policy indicate that it may recognize the need for improvements in these areas.

Management

Numerous agencies have responded to our April 21, 1982, audit

On April 21, 1982, we made major security-related recommendations to OMB, GSA, NBS, and OPM and to the heads of the other executive departments and agencies in our report, "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices." We received responses from 18 agencies, with the major exception of OMB. In January of this year, GSA updated the FPMRs as we had recommended to provide a current cross-reference to the NBS FIPS PUBS on security and related documents. The eighteen agencies generally responded that they shared our security concerns and agreed with our recommendations that agencies conduct risk analyses, incorporate them into new information security programs, and institute internal audits of the programs' implementation. The majority stated they have either taken or planned related action.

Three of the eighteen agencies objected to our major recommendation that OMB revise Circular A-71, Transmittal Memorandum No. 1, to provide more specific guidance on needed controls and on vulnerability assessments of telecommunications

networks. Their concerns focused, in part, on the potential for overcentralization if a revised circular required extensive OMB involvement in the agencies' development and operation of automated information systems.

The central agencies are focusing more attention on information security

The central management agencies are more actively addressing the need for effective federal information security. I mentioned the OMB announcement to revise certain circulars, including Circular A-71, Transmittal Memorandum No. 1, and the update of the FPMRs by GSA. GSA has also issued a temporary FPMR that consolidates government-wide management guidance regarding both automated data processing and word processing technologies. OPM has informed us it will evaluate the issues we raised in our April 1982 report, including the waiver of investigations for certain employees. Finally, NBS has issued and is developing additional FIPS PUBS guidance on information security.

The Financial Integrity Act will foster the development of information security controls

As mentioned, the Financial Integrity Act requires that agencies evaluate internal accounting and administrative controls and that they annually report the results of their evaluations to

the Congress and the President. These agency evaluations must consider the Comptroller General's internal control standards published in 1983.

The Act also requires that internal controls provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. It thus places the administrative, physical, and technical controls used to provide information security squarely within the context of the overall system of agency management's internal controls. The act makes clear the link between the security and management functions and provides a mechanism for security measures to receive renewed emphasis.

DOD information security techniques knowledge could be shared

The Department of Defense (DOD) has been a pioneer in computer and communications security technology for many years and therefore has a wealth of knowledge that could be of benefit to the civil agencies. Let me give a brief background on our work related to the DOD Computer Security Center.

We recommended in an April 5, 1978, report, "Multi-Level Computer Security Requirements of the World Wide Military Command and Control System," that DOD consolidate many of its research and

development activities on computer security. On January 2, 1981, DOD formed the DOD Computer Security Center as a first step in complying with our recommendation. The Center could be a useful resource for civil agencies to consult when conducting computer and communications risk analyses and employing other techniques.

Audits

The President's Council on Integrity and Efficiency is emphasizing audit activities

The President's Council on Integrity and Efficiency, established in March 1981, is taking steps that may improve information security in the federal agencies. The council, chaired by the Deputy Director of OMB, and composed of the Deputy Attorney General, the Director of OPM, and the Federal Bureau of Investigations Executive Assistant Director of Investigations, inspectors general, and other agency designees, is focusing on:

--Standards for the management, operation, and conduct of inspectors general and similar operations in all agencies.

--Efforts to develop a corps of well-trained and highly skilled auditors and investigators.

--Comprehensive plans for government-wide activities attacking fraud and waste.

--Joint projects involving many agencies in special audits and investigations.

An example of the Council's activities in information security is the June 1983 report, "Computer Related Fraud and Abuse in Government Agencies." The report was prepared for the Council by an interagency committee of inspectors general.

SUMMARY

We have attempted in this testimony to underscore the serious nature of computer and telecommunications security vulnerabilities. The potential for loss is increasing because we are concentrating more information--a valuable resource--in automated systems. Also, potential penetrators will have easier access to automated systems using microcomputers, a technology whose sophistication is a long way from peaking.

We have also attempted to provide a balanced perspective on both the information security problems and the potential solutions underway. We wish to emphasize that all agencies have a substantial stake in security and all must contribute to achieving it.

In the policy area, the OMB action to develop a policy circular for federal information management is a positive step and is long overdue. We are not expecting a "cookbook" of absolutes but we do believe a comprehensive policy is needed. It remains problematic what line, if any, should be drawn, between internal control policy and computer security policy; both serve the objective of safeguarding funds, property, and other assets from waste, loss, and unauthorized use.

Recent management actions by the central agencies are encouraging. One of the more formidable challenges will be effective follow-up by OMB in reviewing agency compliance with policy initiatives, particularly those associated with the Financial Integrity Act on internal controls. Equally challenging for the central agencies will be fostering an environment where exchange of information on security techniques between civil and defense sectors can be accomplished.

Although strengthened legislation and policy can serve as aid to improving information security, executive agency action is the most critical factor in terms of its capability to have tangible and timely impact. Agency follow-through on plans for sharpening focus on information security will be a major advance. Likewise, if the agency evaluations of internal controls in response to the Financial Integrity Act afford the appropriate attention to infor-

mation security, all threats alluded to earlier should be minimized. If these evaluations do not address information security controls, however, a crucial opportunity will be lost or, at best, deferred.

The combined impetus provided by the President's Council on Integrity and Efficiency and the inspectors general should bolster internal audit capabilities.

This testimony is not intended to be a complete inventory of the existing or potential information security problems nor does it account for all the progress that is underway. Other developments include OMB efforts to review the agencies' information resources management activities every 3 years as required by the Paperwork Reduction Act. Also, the recent reports of the President's Private Sector Survey on Cost Control, or Grace Committee, called for a stronger government-wide emphasis on information resources management. The Committee called for OMB to exercise more aggressive management leadership. Finally, the administration's Reform 88 program has set a goal of making Federal computer and communications systems more compatible so that waste, fraud, and abuse of programs can be reduced.

To summarize, legislation, policy formulation by the central agencies, and implementation by the executive agencies are key factors in establishing and maintaining a government-wide information security program. Each plays a unique role yet, to be fully effective, they must function as an integrated system.

GAO will be closely monitoring the activities discussed. Currently we are reviewing agencies implementation of the Financial Integrity Act. As part of this effort we will be looking at agencies' vulnerability assessments including those of automated systems.

We welcome all the positive steps taken to date. We must await more tangible evidence of results, however, to determine if the rate of progress is keeping pace with the increasing threats. This completes my prepared remarks. We would be pleased to answer any questions.

SELECTED GAO REPORTS FROM 1976 TO SEPTEMBER 1983 INVOLVING INFORMATION SECURITY OR FEDERAL COMPUTER MATCHING EFFORTS

The two lists in this attachment contain 1) a representative set of 42 GAO reports on major information security issues and 2) 19 representative reports involving federal computer matching efforts. It should be noted that these are not complete listings, since these topics are discussed to some extent in other GAO reports.

REPORTS INVOLVING INFORMATION SECURITY

1. "Need for Internal Control Improvements at ACDA, Including Adequate Internal Audit Coverage" (GAO/NSIAD-83-68, September 30, 1983).

2. "Need to Improve Management of ACDS's Automatic Data Processing and Operations " (GAO/NSIAD-83-66, September 30, 1983).

3. "Computer Technology at IRS: Present and Planned" (GAO/GGD-83-103, September 1, 1983).

4. "Military Services and VA Can Reduce Benefit Overpayments by Improving Exchange of Pay Data" (GAO/AFMD-83-39, July 12, 1983).

5. "Implementing the Paperwork Reduction Act: Some Progress, But Many Problems Remain" (GAO/GGD-83-35, April 20, 1983).

6. "Inadequate Internal Controls Affect Quality and Reliability of the Civil Service Retirement System's Annual Report" (GAO/AFMD-83-3, October 22, 1982).

7. "Analysis of Internal Control Systems to Ensure the Accuracy, Completeness, and Timeliness of Federal Procurement Data" (GAO/PLRD-82-119 September 23, 1982).

8. "Examination of the Social Security Administration's Systems Modernization Plan" (GAO/HRD-82-83, May 28, 1982).

9. "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices" (MASAD-82-18, April 21, 1982).

10. "The Treasury Department and Its Bureaus Can Better Plan for and Control Computer Resources" (GGD-82-9, February 22, 1982).

11. "Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed" (HRD-82-19, December 10, 1981).

12. "The Bureau of the Census Must Solve ADP Acquisition and Security Problems" (AFMD-82-13, October 21, 1981).

13. "Financial Institution Regulatory Agencies Should Perform Internal Audit Reviews of Their Examination and Supervision Activities" (GGD-82-5, October 19, 1981).

14. "Federal Agencies Still Need to Develop Greater Computer Audit Capabilities" (AFMD-82-7, October 16, 1981).

15. "Financial Control System Problems at the Community Services Administration Will Not Be Fully Solved by the Current System Redesign Project" (AFMD-81-96, August 19, 1981).

16. "Weak Internal Controls Make the Department of Labor and Selected CETA Grantees Vulnerable to Fraud, Waste, and Abuse " (AFMD-81-46, March 27, 1981).

17. "Social Security Needs to Better Plan, Develop, and Implement Its Major ADP Systems Redesign Projects" (HRD-81-47, February 6, 1981).

18. "Disappointing Progress in Improving Systems For Resolving Billions in Audit Findings" (AFMD-81-27, January 23, 1981).

19. "Most Federal Agencies Have Done Little Planning for ADP Disasters" (AFMD-81-16, December 18, 1980).

20. "Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies" (LCD-81-1, November 12, 1980).

21. "Weak Financial Controls Make the Community Services Administration Vulnerable to Fraud and Abuse" (FGMSD-80-73, August 22, 1980).

22. "Central Agencies' Compliance With OMB Circular A-71, Transmittal Memorandum No. 1" (LCD-80-56-I, April 30, 1980).

23. "Flaws in Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments" (HRD-79-104, August 9, 1979).

24. "IRS Can Better Plan For and Control Its ADP Resources" (GGD-79-48, June 18, 1979).

25. "Review of DOD's Internal Audits and Policy For Computer Security" (LCD-79-109, March 21, 1979).

26. "Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, January 23, 1979).

27. "The Bureau of Census' Management and Use of ADP Resources" (FGMSD-79-5, December 13, 1978).

28. "VA's New Computer System Has Potential to Protect Privacy of Individuals Claiming Benefits" (HRD-78-135, July 17, 1978).

29. "Procedures to Safeguard Social Security Beneficiary Records Can and Should Be Improved" (HRD-78-116, June 5, 1978).

30. "Inadequacies in Data Processing Planning in the Department of Commerce" (FGMSD-78-27, May 1, 1978).

31. "Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment" (LCD-76-102, April 28, 1978).

32. "Multi-level Computer Security Requirements of the World Wide Military Command and Control System (WWMCCS)" (LCD-78-106, April 5, 1978).

33. "Privacy Issues and Supplemental Security Income Benefits" (HRD-77-110, November 15, 1977).

34. "New Methods Needed for Checking Payments Made by Computers" (FGMSD-76-82, November 7, 1977).

35. "Computer Auditing in the Executive Departments: Not Enough is Being Done" (FGMSD-77-82, September 28, 1977).

36. "IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information" (GGD-77-44, July 11, 1977).

37. "Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, March 31, 1977).

38. "Problems Found With Government Acquisition and Use of Computers From November 1965 to December 1976" (FGMSD-77-14, March 15, 1977).

39. "Safeguarding Taxpayer Information--An Evaluation of the Proposed Tax Administration System" (LCD-76-115, January 17, 1977).

40. "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities" (FGMSD-76-40, May 10, 1976).

41. "Computer Related Crimes in Federal Programs" (FGMSD-76-27, April 27, 1976).

42. "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government" (FGMSD-76-5, April 23, 1976).

REPORTS INVOLVING COMPUTER MATCHING

43. "Computer Matches Identify Potential Unemployment Benefit Overpayments" (GAO/GGD-83-99, August 24, 1983).

44. "Statement of W.D. Campbell, before the Subcommittee on Oversight of Government Management, Senate Committee on Governmental Affairs" (December 16, 1982).

45. "States' Capability to Prevent or Detect Multiple Participation in the Food Stamp Program" (CED-82-103, June 16, 1982).

46. "Prisoners Receiving Social Security and Other Federal Retirement, Disability, and Education Benefits" (HRD-82-43, July 22, 1982).

47. "Millions Could Be Saved By Improving Integrity of the Food Stamp Program's Authorization-To-Participate System" (CED-82-34, January 29, 1982).

48. "Legislative and Administrative Changes to Improve Verification of Welfare Recipients Income and Assets Could Save Hundreds of Millions" (HRD-82-9, January 14, 1982).

49. "States' Efforts to Detect Duplicate Public Assistance Payments" (HRD-81-133, September 17, 1981).

50. "Concerns About HHS' Ability to Effectively Implement Incentive Funding for State Information Systems in the Aid to Families With Dependent Children Program" (HRD-81-119, June 29, 1981).

51. "Impact of State Death Information on Federal Income Security Programs" (HRD-81-113, July 28, 1981).

52. "Millions Can be Saved by Identifying Supplemental Security Income Recipients Owning Too Many Assets" (HRD-81-4, February 4, 1981).

53. "VA Improved Pension Program: Some Persons Get More Than They Should and Others Less" (HRD-80-61, August 6, 1980).

54. "Social Security Should Obtain and Use State Data to Verify Benefits for All Its Programs" (HRD-80-4, October 16, 1979).

55. "Social Security Student Benefits for Postsecondary Students Should be Discontinued" (HRD-79-108, August 30, 1979).

56. "Social Security Should Improve Its Collection of Overpayments to Supplemental Security Income Recipients" (HRD-79-21, January 16, 1979).

57. "Duplicate Payments for Student Benefits Under the Social Security Administration's Retirement, Survivors, and Disability Insurance Program" (HRD-79-27, December 22, 1978).

58. "Letter Report on Duplicate AFDC Payments in New York" (HRD-78-133, June 21, 1978).

59. "Wisconsin's Aid to Families With Dependent Children and Child Support Enforcement Programs Could Be Improved" (HRD-78-130, June 22, 1978).

60. "Privacy Issues and Supplemental Security Income Benefits" (HRD-77-110, November 15, 1977).

61. "Supplemental Security Income Payment Errors Can Be Reduced" (HRD-76-159, November 18, 1976).