

H3962

REPORT BY THE

RELEASED

15410

Comptroller General

OF THE UNITED STATES

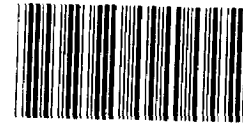
Increasing Use Of Data Telecommunications Calls For Stronger Protection And Improved Economies

The increasing use of data telecommunications networks for transmissions between computer systems and remote terminals heightens the concern about maintaining confidentiality of personal and other sensitive data.

Protection of data transmissions can be strengthened by revising laws pertaining to wiretapping and by strengthening executive level policies and guidelines.

Rapid and uncoordinated growth of data telecommunications in the civil Government has resulted in duplicative and costly dedicated networks.

GAO believes that a properly designed common-user data telecommunications network has the potential for significant savings and improved data transmission protection compared to continued use of certain existing single agency data networks.



113962



LCD-81-1
NOVEMBER 12, 1980

5/28/2

For sale by:

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

Telephone (202) 783-3238

Members of Congress; heads of Federal, State,
and local government agencies; members of the press;
and libraries can obtain GAO documents from:

U.S. General Accounting Office
Document Handling and Information
Services Facility
P.O. Box 6015
Gaithersburg, Md. 20760

Telephone (202) 275-6241



COMPTROLLER GENERAL OF THE UNITED STATES

WASHINGTON, D.C. 20548

B-199052

The Honorable Max Baucus
Chairman, Subcommittee on Limitations
of Contracted and Delegated Authority
Committee on the Judiciary
United States Senate

The Honorable Richardson Preyer
Chairman, Subcommittee on Government
Information and Individual Rights
Committee on Government Operations
House of Representatives

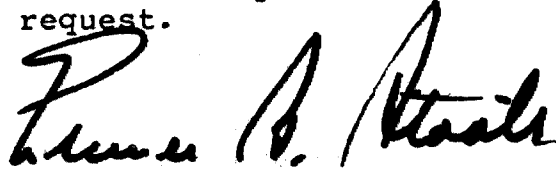
Over the years, we have made many recommendations regarding the adequacy of technical and administrative safeguards for data processing systems used by the Government. We made these recommendations to help Federal agencies improve their data processing operations and save dollars while also safeguarding the privacy of U.S. citizens.

As a related effort, we made this review because the increasing requirements for modern data transmission services in recent years have resulted in a rapid proliferation of costly single purpose or single agency data telecommunications networks in the civil Government. Also, as requested in your August 10 and August 15, 1979, letters (see app. I and II, respectively), we included your questions in our ongoing review of civil agency data telecommunications networks and related privacy issues.

This report recommends that the Congress revise current wiretap law to strengthen its protective provisions. In addition, this report recommends that the Director, Office of Management and Budget, (1) issue additional executive level telecommunications protective policies and guidelines for data transmissions containing personal data and (2) make a comprehensive study to provide the Congress with accurate information on the merits and problems of implementing a common-user data telecommunications network for the civil Government.

B-199052

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of the report. At that time we will send copies to interested parties and make copies available to others upon request.

A handwritten signature in black ink, appearing to read "Thomas A. Stearns". The signature is written in a cursive style with a large initial 'T' and 'S'.

Comptroller General
of the United States

D I G E S T

The Government's increasing use of telecommunications to extend data processing systems raises a variety of new issues and management problems concerning the protection of data transmissions against unauthorized, unwarranted, and illegal uses. (See p. 2.)

A major concern of the Congress is to maintain the confidentiality of vast amounts of personal and other sensitive information collected, maintained, and disseminated by Federal agencies. (See p. 1.)

Machine generated communications that are being transmitted over interstate and foreign telecommunications facilities are not protected by current laws against unauthorized interceptions. Protection of data telecommunications against unauthorized wiretapping can be strengthened by amending telecommunications laws. GAO believes the 1968 Crime Control Act should be revised to extend its protection to all forms of electronic transmissions. (See pp. 6 to 9.)

Civil Government agencies need guidance to determine appropriate safeguards and controls for telecommunications. Although telecommunications are used to extend data processing systems to remote locations, executive level policies and guidance on telecommunications provide little assistance for operating agencies. (See pp. 12, 15, 16, 18, and 20.)

GAO believes that previous reviews on data processing showed that controls on Federal users and others authorized to collect and handle personal information should be strengthened to increase privacy protection for personal and other sensitive information, regardless of whether shared transmission facilities and related network controls are used. (See p. 32.)

LCD-81-1

Data telecommunications networks in the civil Government are generally acquired from commercial telecommunications carriers by individual agencies for their own exclusive use. Estimated costs for civil agency networks range from \$100 to \$200 million annually. Some departments and agencies have taken or are taking actions to reduce their transmission costs through circuit sharing. (See pp. 35, 39, and 40.)

On the basis of savings already achieved through circuit sharing by certain agencies and projected for other agencies, GAO believes the consolidation of certain civil Government data telecommunications into a shared data telecommunications network could potentially reduce total Federal data telecommunications costs by at least 20 percent. (See p. 35.)

GAO believes that significant Government savings can be achieved through use of common user data telecommunications technology without conflicting with privacy objectives. Therefore, a comprehensive civil Government telecommunications study should be made to show complete and accurate information on (1) a preliminary network design with the levels of economy achievable, (2) the extent of privacy protection, (3) the implications on the telecommunications industry, and (4) the proposed management arrangements. (See pp. 41 and 42.)

RECOMMENDATIONS

GAO recommends that the Director of the Office of Management and Budget, in cooperation with the Secretary of Commerce, direct the Administrator, National Telecommunications and Information Administration, to develop clear policy guidelines and standards for Government data transmissions protection. These guidelines and standards should:

--Be consistent with the computer security guidance published by the National Bureau of Standards for automated data processing.

--Require risk analyses for data telecommunications networks supporting data processing systems used to maintain personal or other sensitive data.

--Include standards and implementing guidelines for determining the appropriateness of encoding data with encryption techniques for electronic transmissions, including those containing personal information. (See p. 25.)

The agencies commenting on the draft of this report have varying views on whether current executive level guidance on telecommunications protection is adequate. (See p. 25.)

GAO also recommends that the Director, Office of Management and Budget, take appropriate action, including seeking concurrence from appropriate congressional oversight committees, to have a study made of the merits and problems of proceeding with a shared civil Government data telecommunications network instead of continuing with separate dedicated networks. In fulfilling that task, the Director, Office of Management and Budget, with the assistance of the Administrators of General Services and the National Telecommunications and Information, should provide to the appropriate congressional oversight committees complete and accurate information on a potential shared data telecommunications network for the civil Government. This study should include the levels of economy achievable; the provisions for privacy protection; the implications on industry and Federal policies for the kind of procurement, ownership, and management controls proposed; and the impact on the affected civil agencies' data telecommunications cost and operations. (See p. 43.)

Some of the agencies commenting on this report questioned whether network controls for a common-user network would provide better privacy protection than controls in existing dedicated networks. However, none disputed the fact that

privacy implications of data transmissions should not be a deterrent from achieving potential economies by implementing a common-user telecommunications network. (See p. 32.)

Most agencies agreed that there were certain potential economical advantages of implementing a common-user data telecommunications network, but stated that the savings GAO projected could not be verified without making a comprehensive study as recommended. The General Services Administration had already initiated actions consistent with GAO's recommendations. It completed a preliminary study with the consent of its legislative oversight committees which indicated that a common-user network could satisfy a large number of civil Government agencies requirements with increased performance at a lower cost. Also, its report recommended a comprehensive study in line with GAO's recommendations above. (See pp. 44 and 45.)

RECOMMENDATIONS TO THE CONGRESS

Several bills have been introduced into the Congress to amend or rewrite the 1934 Communications Act and to amend the 1968 Crime Control Act. In considering these bills, GAO recommends that the Congress revise existing or proposed legislation to provide protective provisions against unauthorized interception of all forms of telecommunications, not just those forms limited to aural acquisition. (See p. 9.)

The Office of Management and Budget and the National Telecommunications and Information Administration agree that legislative revisions are needed to strengthen the protection provided by the current wiretap law. Also, the need to address past concerns of the law enforcement and intelligence agencies with such revisions is pointed out. (See pp. 9 and 10.)

The Congress should limit the development and implementation of dedicated data telecommunications networks pending completion of the study and congressional determination on whether to proceed with a shared civil Government data telecommunications network. (See p. 44.)

C o n t e n t s

		<u>Page</u>
DIGEST		i
CHAPTER		
1	INTRODUCTION	1
	Growth and variety of data telecommunications used by civil agencies	2
	Civil Government communications management organizations and responsibilities	3
	Objectives, scope, and methodology	5
2	STRENGTHENED TELECOMMUNICATIONS LAWS COULD ENHANCE DATA CONFIDENTIALITY	6
	Improved telecommunications protection laws could strengthen confidentiality of personal data transmissions	6
	Recommendation to the Congress	9
	Agency comments and our evaluation	9
3	FEDERAL CIVIL AGENCIES NEED GUIDANCE ON DATA TELECOMMUNICATIONS PROTECTION	11
	Data telecommunications network-- a distinct part of civil automated information systems	12
	Executive level policy guidance needs strengthening	14
	Conclusions	24
	Recommendations	25
	Agency comments and our evaluations	25
4	PRIVACY IMPACT OF SHARED DATA TELECOMMUNICATIONS FACILITIES AND ASSOCIATED NETWORK CONTROLS	27
	Comparison of dedicated and shared network vulnerabilities	28

CHAPTER		<u>Page</u>
	Comparison of shared versus dedicated network controls to prevent misuse	29
	Conclusions	31
	Agency comments and our evaluation	32
5	SHARED DATA TELECOMMUNICATIONS NETWORK--A POTENTIAL FOR SIGNIFICANT SAVINGS	34
	Proliferation of dedicated networks	34
	Economical potential of sharing	36
	Conclusions	43
	Recommendations	43
	Agency comments and our evaluation	44
 APPENDIX		
I	Letter dated August 10, 1979, from the Chairman, Subcommittee on Government Information and Individual Rights, House Committee on Government	46
II	Letter dated August 15, 1979, from the Chairman, Subcommittee on Limitations of Contracted and Delegated Authority, Senate Committee on the Judiciary	48
III	Letter dated August 7, 1980, from the Assistant Director, Regulatory and Information Policy, Office of Manage- ment and Budget	50
IV	Letter dated July 22, 1980, from the Administrator of General Services	54
V	Letter dated August 8, 1980, from the Inspector General, Department of Commerce	55
VI	Letter dated July 17, 1980, from the Assistant Attorney General for Administration, Department of Justice	59

APPENDIX

Page

VII	Letter dated July 21, 1980, from the Director, Office of Operations and Finance, Department of Agriculture	61
VIII	Letter dated July 22, 1980, from the Assistant Secretary for Policy, Budget and Administration, Department of the Interior	64
IX	Letter dated July 28, 1980, from the Assistant Secretary for Administration, Department of the Treasury	66
X	Letter dated July 23, 1980, from the Executive Vice President, U.S. Independent Telephone Association	67
XI	Letter dated July 18, 1980, from the Chairman, Procurement Committee, Association of Data Processing Service Organization	

ABBREVIATIONS

ARS	Advanced Record System
DES	Data Encryption Standard
FEDNET	Federal Information Network
FTS	Federal Telecommunications System
GAO	General Accounting Office
GSA	General Services Administration
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget



CHAPTER 1

INTRODUCTION

One major concern of the Congress is to maintain the confidentiality of vast amounts of personal and sensitive information collected, maintained, and disseminated by Federal agencies. Often this information is stored in data processing computers connected to remote terminals via data telecommunications networks which are generally procured individually by the respective agencies. While recognizing the need for economy and efficiency in handling, processing, and transmitting information, the Congress has demonstrated that a greater priority rests in keeping the public trust of privacy. The following are examples which illustrate this concern.

The House Committee on Government Operations 1968 report 1/ summarized the congressional response to a proposed National Data Center. The Committee concluded that the data center posed serious problems regarding the collecting, using, and sharing of personal information. It strongly advised against establishing the data center until the technical feasibility of protecting automated files could be fully explored and privacy could be guaranteed.

The proposed joint General Services Administration (GSA) and Department of Agriculture computer resource sharing and data telecommunications project, labeled FEDNET, met similar congressional opposition. Data base sharing proposed by GSA and Agriculture was limited to only Agriculture information. However, since the Congress had not been fully informed of the project plans and computer resource sharing was involved, there was widespread concern that the project could be expanded to bring together various computer data bases containing privacy information without adequate data processing controls. As a result, GSA canceled its portion of the project in July 1974. We were also concerned with the data processing controls in Agriculture's portion of the project and pointed out deficiencies in its procurement planning in our June 1975 report

1/Hearing before a Special Subcommittee on Invasion of Privacy, House Committee on Government Operations, 89th Cong., 2 sess. (1966), p. 3.

to the Congress 1/. As a result, the Congress imposed limitations on spending, and Agriculture canceled its planned procurement in October 1975.

Congressional concerns for privacy were later expressed when the Internal Revenue Service proposed the Tax Administration System. This proposed project differed significantly from the proposed National Data Center and FEDNET in that telecommunications linkage and computer sharing with other agencies were not involved. We pointed out in our report 2/ to the Congress that this system, through proper design and implementation, would be able to provide a high level of protection for taxpayer information, but selected data processing controls were needed. The Internal Revenue Service terminated this system because of congressional disapproval, with privacy as one of the major issues.

The Federal Bureau of Investigation has repeatedly run into congressional opposition to its proposal for an automated telecommunications switch. The Congress was concerned about the potential misuse of the switch to obtain messages not destined to nor intended for use by the Bureau.

GROWTH AND VARIETY OF DATA TELECOMMUNICATIONS USED BY CIVIL AGENCIES

We were unable to obtain reliable cost information on total data telecommunications used by the civil Government, but estimates of annual costs ranged from \$100 million to \$200 million. Likewise, we could not obtain growth rate projections. The most reliable estimates were between 10 and 25 percent cumulative annual increases.

The Government's widespread and increasing use of data telecommunications networks to extend data processing systems affects nearly every facet of today's Government administration. A variety of new issues and management problems evolved with the growth of these technologies. The protection of data transmissions against unauthorized, unwarranted, and illegal acts has become a major challenge.

1/"Improved Planning--A Must Before a Department-wide Automatic Data Processing System is Acquired for the Department of Agriculture" (LCD-75-108, June 3, 1975).

2/"Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, Jan. 17, 1977).

The growth of data telecommunications networks in the civil Government is characterized as being rapid and uncoordinated. These telecommunications networks are generally acquired from commercial telecommunications carriers by individual agencies for their own use. Also, the existing shared common-user telecommunications networks, which GSA administers, provide data telecommunications services for civil Government agencies. For example:

--The Federal Telephone System, which was initiated in 1964 primarily to provide long-distance telephone service, is used by many agencies today to transmit data.

--The Advanced Record System (ARS), which was established in 1966 to provide narrative message communications services, basically provides some slow speed data services between agency computers and their associated remote terminals.

Because the capability of these existing common-user telecommunications networks is limited in modern automated information systems, separate telecommunications services for use by individual agencies are proliferating rapidly. (See ch. 5.)

CIVIL GOVERNMENT COMMUNICATIONS MANAGEMENT ORGANIZATIONS AND RESPONSIBILITIES

No single Federal agency reviews and coordinates total civil Government telecommunications plans and requirements. Formulation of telecommunications policy is similarly fragmented and diluted.

Until March 1978 the Office of Telecommunications Policy was the primary focal point for telecommunications policy in the Government. At that time, the Office was abolished and its functions were distributed to several organizations, including the Office of Management and Budget (OMB), the President's National Security Council, and the Department of Commerce.

Office of Management and Budget

Under the March 1978 Executive Order 12046, OMB became responsible for advising the President on policies relating to Federal telecommunications systems and developing and establishing policies for such systems.

Department of Commerce

That Executive order also gave the Department of Commerce several responsibilities. These responsibilities include studying and evaluating Federal telecommunications systems and advising the Director, OMB, on policies for such systems. Specifically, these responsibilities include considerations of interoperability, privacy, security, radio frequency spectrum use, and emergency readiness.

General Services Administration

The Federal Property and Administration Services Act of 1949 (40 U.S.C. 481) gives the Administrator of General Services the responsibility for procuring and supplying general-purpose telecommunications services for civil Government agencies. The Administrator is also responsible for assuring that telecommunications services, which GSA procures for civil agencies, meet the user agencies security requirements and are consistent with the Privacy Act of 1974.

User agencies

Agencies are responsible for managing their telecommunications activities. Responsibilities include (1) planning and acquiring services through GSA or directly from vendors by delegation of procurement authority from GSA and (2) determining special requirements, if any, for administrative, technical, and physical safeguards and controls to protect the confidentiality of data telecommunications.

Commercial telecommunications carrier companies

Commercial telecommunications carrier companies are responsible for furnishing telecommunications services to the Federal Government upon reasonable request and in accordance with rules established by the Federal Communications Commission and State regulatory bodies. According to officials from commercial carrier companies and the Government, information users are responsible for determining the means necessary to protect the privacy and security of information which is transmitted over commercial carrier networks. In this study, we made no attempt to determine what the relative responsibilities of commercial carriers and users ought to be.

OBJECTIVES, SCOPE, AND METHODOLOGY

Several of our reports have addressed areas of computer security for data processing applications and attendant privacy safeguards. This report is our first comprehensive attempt to cover civil Federal agency data telecommunications networks and their transmission protection safeguards and controls. In this report, we have (1) identified a need to extend the protective provisions of current laws to all forms of unauthorized interceptions, (2) pointed out omissions in Federal telecommunications policy guidance, (3) addressed certain privacy implications of sharing transmission facilities, and (4) pointed out that shared data telecommunications networks have the potential for significant savings for the Government.

During this review, we evaluated documents and agency responses to our telecommunications controls questionnaire and interviewed officials in OMB, the Departments of Agriculture, Commerce, Energy, Health and Human Services, the Interior, Justice, and the Treasury; GSA; the Veterans Administration; the Federal Reserve Board; and the National Communications System. We also interviewed officials from several commercial telecommunications and computer companies.

We provided draft copies of this report to 11 agencies and 3 industry associations for review and comment. We received comments from the Departments of Agriculture, Commerce, the Interior, Justice, and the Treasury; OMB; GSA; and two industry representative organizations--the Association of Data Processing Service Organizations and the U.S. Independent Telephone Association. (See apps. III, to XI.)

Corrections and clarifications of facts and statements in our draft suggested by the respondents have been incorporated into this final report, where necessary and appropriate.

CHAPTER 2

STRENGTHENED TELECOMMUNICATIONS

LAWS COULD ENHANCE DATA

CONFIDENTIALITY

During this review we evaluated existing and proposed laws on telecommunications to determine whether additional legislation was needed to protect electronic transmissions containing personal information.

In our study of existing legislation, we concentrated on the Communications Act of 1934, as amended, the Omnibus Crime Control and Safe Streets Act of 1968, the Privacy Act of 1974, and the Foreign Intelligence Surveillance Act of 1978. Our study of proposed legislation included the Communications Act rewrite bills.

In our opinion, the protective provisions in existing and proposed laws concerning interceptions of electronic transmissions, which may also include personal or other unclassified sensitive information, can be improved to strengthen protection against unauthorized wiretapping. Specifically, current statutory protection against unauthorized interception does not apply to all wiretapping techniques.

Since the existing leased or owned telecommunications facilities used by civil Government agencies are generally considered susceptible to wiretapping, such protection could be in the interest of minimizing potential invasions of individual privacy of people or firms served by the Government.

IMPROVED TELECOMMUNICATIONS PROTECTION LAWS COULD STRENGTHEN CONFIDENTIALITY OF PERSONAL DATA TRANSMISSIONS

The comprehensive statutory provisions prohibiting unauthorized interceptions of radio and wire communications originally provided by the Communications Act of 1934 were modified in 1968. As a result, current wiretap laws do not prohibit unauthorized interceptions when nonaural wiretapping techniques are used. Nonaural wiretapping includes the use

of machines or similar means to intercept transmissions. Because of advancing technologies, more machine generated communications, possibly including digitized voice in non-aural form, are being transmitted which are not protected by current laws against unauthorized interceptions.

Originally, the Communications Act of 1934 contained comprehensive statutory provisions on wiretapping. This act covered voice and nonvoice communications; that is, writings, signs, signals, pictures, and all sounds transmitted over interstate and foreign wire and radio telecommunications media. Section 605 of the act prohibited persons not authorized by the sender to intercept 1/ interstate or foreign communications transmitted over wire or radio.

The 1934 act's comprehensive protective provisions on wiretapping were modified by the enactment of the Omnibus Crime Control and Safe Streets Act of 1968. 2/ This modification did not change the 1934 act's protection against unauthorized interception of radio communications, but it did alter the 1934 act's statutory protection for wire communications against unauthorized wiretapping.

The 1968 Crime Control Act used the qualifying term "aural acquisition" (acquired by use of the ear or sense of hearing) in its definition of interception. As a result, only interceptions made by aural means are illegal, except by court order. Nonaural interceptions (acquisition by use of devices or equipment) are no longer illegal.

Advancing telecommunications technologies which involve nonaural interception techniques are being used more; therefore, modern telecommunications are becoming less likely to be protected against unauthorized interception by current statutory provisions. For instance, telecommunications links connecting data terminals and computer equipment for data transmission are increasing rapidly. Nonaural interception of these data transmissions can be accomplished by similar data terminals and computer equipment. Thus, it is not

1/The term "intercept" was not defined in the 1934 act. However, as used in section 605, the term implies the unauthorized acquisition or interception by any means.

2/Public Law 90-351, title III, sec. 803, 82 Stat. 223.

illegal to intercept data communications, such as telegrams and teletype messages, or computer data, or facsimile and television transmissions, which may include personal information.

Also, within the current state-of-the-art technologies, more voice transmissions are being converted to pulse-coded tones or a digital language form by telecommunications equipment for transmissions. These transmissions may be intercepted from wire communications facilities using non-aural means, such as digital receiving machines and equipment. However, on the basis of our review of technical literature and the 1968 Crime Control Act and on our interviews with telecommunications experts, we could not conclude whether wiretapping to acquire digitized voice transmissions was or was not excluded from this law. Since this law defines "interception" as the aural acquisition of the contents of any wire or oral communications, it is not entirely clear whether interception of a digitized voice transmission is considered an aural acquisition. In other words, inasmuch as voice transmissions in these instances are not strictly aural forms, but rather pulse-coded tones, it may be reasonably argued that such interceptions are outside the purview of aural acquisition.

The protective provisions of current legislation should be a major concern because telecommunications facilities are vulnerable to wiretapping techniques. As pointed out in our report "Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, Mar. 31, 1977), all the transmissions of a user are available from local access lines. These lines, generally wire cables routed from a user's premise to local commercial telecommunications centers, are the optimum places for interception. In addition to eavesdropping on user transmissions, a wiretapper can penetrate these access lines to acquire information, such as a dial-up number or an access code to a computer. The wiretapper can then use the dial-up number to gain access to a computer, defeat the computer's access controls, and surreptitiously take information from the user's confidential data bases. We found two such cases in literature about computer fraud.

Therefore, we concluded that (1) the protective statutory penalties of the 1934 Communications Act, as amended, may not be applicable to interceptions from wire

communications and (2) 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 (possibly including digitized voice) carried over wire transmission facilities without a court order and not be in violation of the law.

RECOMMENDATION TO THE CONGRESS

Several bills have been introduced into the Congress to amend or rewrite the 1934 Communications Act and to amend the 1968 Crime Control Act. In revising these bills, we recommend that the Congress provide protective provisions against unauthorized interception of all forms of telecommunications, not just those forms limited to aural acquisition. Of course, this legislation must be consistent with:

- The rights of individuals embodied in the U.S. Constitution.
- The need to protect copyrighted, proprietary, and other similiar information transmitted via telecommunications systems.
- The legislative mandated missions of Federal agencies involving national security, foreign affairs, domestic and foreign intelligence, and law enforcement.
- The modern wire and radio transmission technologies used for both voice and data telecommunications.

A direct and simple way to improve the protective provisions would be to clarify the definition of "intercept" in the 1968 Crime Control Act.

AGENCY COMMENTS AND OUR EVALUATION

GSA endorsed our recommendations. The National Telecommunications and Information Administration (NTIA) strongly supported our recommendation for correcting the deficiencies in the current wiretap law. It suggested that we should address previous objections to bans on electronic surveillance voiced by intelligence and law enforcement agencies because certain electronic surveillance was needed for law enforcement and national security.

The scope of our review did not include assessments of previous objections presented during the congressional hearings on the 1968 Crime Control Act. However, we noted certain compromises were granted for law enforcement, such as court authorized wiretaps. Also, our recommendation considers the missions of certain Federal agencies which allows the Congress to incorporate exceptions, where it deems appropriate, for law enforcement and intelligence agencies.

OMB agreed that the current wiretap law needed strengthening, but recommended that it may be more appropriate to incorporate amending provisions in Senate Bill 240 (Federal Computer Systems Protection) which is currently being considered by the Congress.

Although the Congress may also consider OMB's recommendation, we believe revising the 1968 Crime Control Act is more appropriate because revision to the 1968 act will provide protective provisions for both voice, including digitized voice, and data transmissions, including noncomputer generated transmissions, over wire communications facilities. Also, Senate Bill 240 does not apply to most private companies.

CHAPTER 3

FEDERAL CIVIL AGENCIES NEED GUIDANCE

ON DATA TELECOMMUNICATIONS PROTECTION

Our evaluations of selected civil agencies' data telecommunications networks indicated that these agencies had not properly addressed in their security programs the vulnerabilities of these networks. Specifically, we found that their programs usually did not include appropriate risk analyses of their data telecommunications networks to determine (1) the vulnerabilities to which data flowing through the telecommunications network were exposed, (2) the proper safeguards and controls needed for data transmissions which might contain personal information, and (3) whether the cost of encrypting data transmissions was warranted based on transmission vulnerabilities and the value of the data transmitted. We also found that executive level direction and guidance was not adequate for assisting such determinations by civil Government agencies.

On the basis of the documentation provided on various agencies' data telecommunications networks, we found that agencies had given little attention to determining appropriate safeguards and controls for the data telecommunications networks supporting agency data processing systems. Agency safeguards and controls were basically for only the use of data processing resources and data files. Since an indepth risk management analysis would be required on a case-by-case basis, we did not determine whether agency data telecommunications network vulnerabilities warranted strengthening the data processing safeguards and controls. However, on the basis of responses to our questionnaire on telecommunications controls, we believe that additional improvements may be needed to enhance the protection of agencies' unclassified data transmissions, including those containing personal and other sensitive data.

We have made various studies of Federal computer systems and the adequacy of agency security programs to protect private information. A recent report entitled "Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, January 23, 1979), pointed out that:

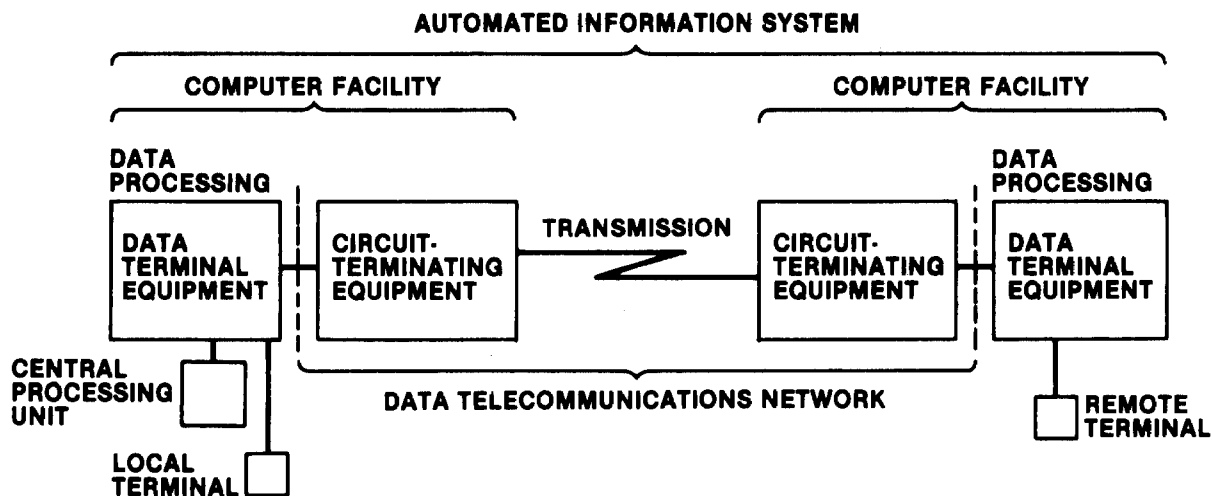
"* * * Agencies usually had selected computer safeguards intuitively rather than on a cost effectiveness determination which would take into account the degree of sensitivity and vulnerability of the information to be protected."

After completion of that study, OMB issued additional guidelines on computer security for Federal automated information systems which require action by agency managers. These guidelines, if properly implemented, could contribute greatly to correcting many of the data processing problems referred to in our January 1979 report. We have initiated a followup review to determine whether those guidelines are being implemented. However, these additional guidelines are oriented primarily toward computer security for data processing systems and are not specifically directed toward telecommunications networks supporting such systems.

While our previous studies have focused on policies and procedures of data processing activities, this study focuses on the adequacy of Federal policies and guidance for data telecommunications systems.

DATA TELECOMMUNICATIONS NETWORK--A DISTINCT PART
OF CIVIL AUTOMATED INFORMATION SYSTEMS

Civil Government data telecommunications networks are generally similar in structure and characteristics. For the most part, they consist of the transmission and switching facilities of public telecommunications systems. Our evaluations show that most civil agency data telecommunications networks are an intrinsic part of automated information systems. However, these networks can generally be evaluated as a separate entity for purposes of identifying telecommunications vulnerabilities. As the following illustration shows, except for the functions necessary to interconnect data circuit terminating equipment with data processing terminal equipment, the data telecommunications network portion of an automated information system is a functionally separate entity.



This separation requires independent vulnerability assessments of the data telecommunications networks in terms of the functions to be performed (signaling, switching, and transmitting) and the equipment and facilities to be used.

These independent assessments form the basis for determining telecommunications vulnerabilities and the impact these vulnerabilities have on

- the safeguards and controls which have been implemented in the data processing portion of an automated information system and
- the integrity of electronic transmissions flowing through the data telecommunications network portion of the system.

Once these are known, an agency's management can determine what safeguards and controls are appropriate for data processing and transmission facilities, which of these safeguards and controls need strengthening, and what new measures need to be added, if any.

EXECUTIVE LEVEL POLICY GUIDANCE NEEDS STRENGTHENING

The advancements of telecommunications technology, changes in legislative and regulatory policies, and the integration of telecommunications and data processing functions demand continuing policy direction at the highest level in the Federal Government. Although telecommunications is not specifically addressed in the Privacy Act of 1974, three sections of the act imply that Federal agencies can be held responsible if vulnerabilities in telecommunications networks adversely affect data processing systems which are used to maintain personal records.

Generally, civil agencies lack executive level guidance for assessing data telecommunications vulnerabilities. This guidance is necessary to determine whether telecommunications controls are adequate to protect personal information flowing through the agencies' data telecommunications networks, or whether encryption techniques are warranted for such transmissions.

The responsibility for telecommunications policy resides with OMB and the Department of Commerce's NTIA. OMB's responsibility for telecommunications policy, contained in Executive Order 12046, includes developing and establishing policies for procurement and management of Federal telecommunications systems.

Executive Order 12046 also specifies NTIA's responsibilities. Pertinent to this review, these responsibilities include

- advising OMB on policy development relating to the procurement and management of Federal telecommunications systems;
- making studies and evaluations, including initiation, improvement, and use of Federal telecommunications systems, and advising OMB of recommendations resulting from such studies and evaluation; and
- formulating and coordinating telecommunications policy for the executive branch, including policy guidance for privacy and security.

Limitations of existing executive level directives

During our review, we found only three executive level directives on telecommunications protection for unclassified data transmissions. These were:

- OMB Circular A-108, Transmittal Memorandum No. 5, Policy Responsibility for Government Telecommunications under the Privacy Act (August 3, 1978);
- OMB Circular A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems (July 27, 1978); and
- Presidential Directive/National Security Council (PD/NSD) 24 (unclassified extract), National Telecommunications Protection Policy (February 16, 1979).

These directives contained only limited telecommunications guidance for civil Government agencies to use in determining appropriate safeguards to protect personal and proprietary data, as discussed in the following sections.

OMB Circular 108, Transmittal Memorandum No. 5

Under OMB Circular A-108, the Director, OMB, is responsible for revising and issuing policies and guidelines, in consultation with NTIA, on Government data telecommunications relative to the Privacy Act of 1974. ^{1/} However, OMB officials told us that they considered the guidelines issued under Circular A-71 were also intended for telecommunications. NTIA officials told us that they had no ongoing effort for developing telecommunications protection policy standards and guidelines for personal data transmissions. In addition, NTIA officials said the only practical solution to the Privacy Act requirements was through agency administration controls that restricted use and distribution of personal data by users of automated information systems.

^{1/}The former Office of Telecommunications Policy was originally delegated this responsibility under OMB Circular A-108. However, Executive Order 12046 abolished this Office and its responsibility was assumed by OMB under Circular A-108, Transmittal No. 5, dated August 3, 1978.

We believe that, although telecommunications is not specifically addressed, three sections of the Privacy Act of 1974 state that Federal agencies are responsible for accurate maintenance and appropriate safeguards to records, as well as the establishment of rules of conduct for persons involved in maintaining record systems. These sections imply that agencies are responsible for vulnerabilities in telecommunications networks used to support agency systems containing personal data.

OMB Circular A-71, Transmittal Memorandum No. 1

This circular, hereafter called Circular A-71, T1, requires each Federal agency with automated information systems to implement computer security programs and report its progress to OMB. However, Circular A-71, T1, does not contain direction and guidelines for assessing telecommunications vulnerabilities and for including these vulnerability assessments in agency security programs.

We reviewed five civil agency reports to OMB in response to Circular A-71, T1. These reports showed that the agencies' programs did not provide for assessing telecommunications vulnerabilities and including the impact of vulnerabilities on the data processing system safeguards and controls. Generally, agency officials responsible for data telecommunications security that we interviewed believed that their safeguards and controls for computer facilities, including remote user terminals, met OMB Circular A-71, T1, requirements for protecting data within their data processing systems. However, safeguards and controls for protecting computer facilities often do not protect against vulnerabilities in telecommunications networks supporting such systems. Therefore, we believe that agency programs for assessing safeguards and controls of a total automated information system should specifically address the data telecommunications portion of the system.

OMB officials did not believe that additional guidance on telecommunications was needed to assist Federal agencies in implementing comprehensive security programs for automated information systems. However, they did agree that data telecommunications networks, which are primarily vehicles for transmitting personal and other sensitive information within and between civil government agencies and among these agencies and the private sector, could significantly affect the adequacy of safeguards agencies are planning for the data processing portion of their automated information systems.

Presidential Directive 24

This Presidential Directive established a new national telecommunications protection policy. Although this directive is classified, an unclassified extract entitled "National Telecommunications Protection Policy," dated February 16, 1979, shows that the responsibilities for developing telecommunications policy guidelines are assigned to the Secretary of Defense as executive agency for communications security (the Director, National Security Agency, delegated authority) and to the Secretary of Commerce as executive agent for communications protection (the Administrator, NTIA, delegated authority). 1/ This directive states, in part, that:

- Government classified information on national defense and foreign relations shall be transmitted only by secure means.
- Unclassified information transmitted by and among Government agencies and contractors that would be useful to adversaries should be protected.
- Nongovernmental information that would be useful to any adversary shall be identified and the private sector informed of problems and encouraged to take appropriate measures.
- As a precautionary measure, the responsible agencies should work with the Federal Communications Commission and the common carriers to adopt system capabilities which protect the privacy of communications and to carry out changes in regulatory policy and draft legislation that may be required.

We commend these policy objectives. The first objective reaffirms the need for continued secure protection of electronically transmitted national defense and foreign affairs information. We believe the last three new objectives are long needed for countering the efforts of certain foreign and domestic individuals that surreptitiously penetrate and exploit unclassified sensitive information flowing through U.S. national telecommunications networks.

1/The National Security Council's Special Coordination Committee is responsible for policy guidance and for implementation of Presidential Directive 24.

However, the responsibilities assigned to develop guidelines for the fourth objective are not clear. Officials of common carrier companies told us that the responsibility for determining privacy and security protection requirements belonged to the users. They also said that their companies would not assume that responsibility.

Also, since NTIA has not considered electronic transmissions containing personal data useful to adversaries, it has no ongoing effort to develop guidelines for protecting personal data in the telecommunications environment. Rather, NTIA's effort to formulate telecommunications protection guidelines for unclassified transmissions has been placed exclusively on information, such as

- financial information, including planned changes in prime interest rates and the support of the dollar in foreign exchange markets;
- commodity market forecasts;
- supply of critical materials;
- strategies for international negotiations; and
- selected high-technology information.

Therefore, it is not clear whether NTIA will formulate telecommunications guidance for electronic transmissions when only personal information is involved.

On the basis of our evaluation of executive policy directives discussed above, there is neither specific telecommunications policy direction and guidance nor ongoing efforts to develop such guidance to assist Federal agencies to determine the threats posed to personal data in data telecommunications environments. As a result, Federal civil agencies lack guidance needed for comprehensive risk management.

Telecommunications protection guidance should include risk analyses

All of the civil Government agencies we reviewed had initiated computer security programs and had plans for the data processing portion of the automated information systems

as required by OMB Circular A-71, T1. However, because of the lack of specific direction and guidance in this memorandum, agency security programs and plans did not specifically include risk analyses of data telecommunications vulnerabilities. These analyses are necessary for selecting appropriate safeguards and controls for information transmitted to and from data processing systems.

A risk analysis for data telecommunications networks consists of identifying vulnerabilities to which electronic data are exposed and estimating the potential adverse effects associated with each identified vulnerability. It is complicated because of the nature of the threats to which a data telecommunications network may be subjected, the potential benefit to be gained, and the cost of subverting or penetrating the network.

OMB Circular A-71, T1, requires agencies to make risk analyses for data processing systems. The National Bureau of Standards issued the implementing guidelines entitled "A Guideline for Automatic Data Processing Risk Analysis" (Federal Information Processing Standards Publication-FIPS PUB 65, dated August 1, 1979). These guidelines specifically require agencies to make risk analyses for data processing facilities. However, they do not specifically require risk analyses for data telecommunications networks. Therefore, as pointed out previously, we believe agencies did not require their computer security plans to specifically include risk analyses for their data telecommunications networks because there was a lack of executive level direction and guidelines.

Specific guidance on use of encryption
for personal data is needed

Encryption for telecommunications is expensive; therefore, it is important that a definite need be established, through a formal threat analysis, before an agency decides to use this technology. Transmissions containing highly sensitive or confidential data are most likely to need encryption. Transmissions containing financial transactions or other critical data may also need encryption, especially if, a threat assessment indicates that enough benefits can be derived from intercepting such transmissions to compensate for the risk and the cost of such an effort.

There is a growing interest in civil Government agencies to encrypt data transmissions containing personal information. However, these agencies lack executive level guidance to make threat assessments of their data telecommunications networks. We believe that cryptography should only be used to secure telecommunications links after an agency has determined through a risk analysis and a threat assessment that the vulnerabilities of a given data telecommunications network are unacceptable.

Our report entitled "Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, March 31, 1977) noted that telecommunications systems were vulnerable to various penetration and interception techniques that might be used for (1) gaining access to systems and (2) intercepting communications traffic carried over systems or inserting traffic onto the systems. The report further noted that the difficulty of penetration was dependent upon such factors as the adequacy of administrative controls, the competence and integrity of telecommunications personnel, the physical security maintained over telecommunications facilities, the technical security resulting from telecommunications technology, and the penetrator's technical knowledge and financial resources.

Cryptography involves using an encryption device at the point of data transmission and a decryption device at the point of data reception. Therefore, these devices and related control equipment are required at all remote terminals or terminal controllers, as well as at computer facilities.

On January 15, 1977, the National Bureau of Standards published the Data Encryption Standard (DES) (Federal Information Processing Standard Publication 46). DES specifies an algorithm to be implemented in electronic hardware devices used for the cryptographic protection of computer data. 1/ DES became effective on July 15, 1977, and applies to all Federal data processing systems when agencies determine that cryptographic protection is required.

1/DES is actually an algorithm. Its logic is implemented using microelectronic techniques by circuitry in tiny electronic components called chips. These chips are incorporated with hardware circuitry of data processing or telecommunications equipment.

A Federal committee responsible for establishing Federal telecommunications standards is developing a telecommunications standard for DES. This standard will specify compatibility related requirements regarding DES use in Federal data telecommunications. However, this standard is not intended to provide guidance for determining when cryptographic protection for data transmission is required.

Furthermore, we found no executive level guidance for determining when use of encryption techniques to protect transmissions containing personal and other unclassified sensitive data is required. The National Bureau of Standards has drafted guidance entitled "Security for Computer Applications" to assist agencies in implementing OMB Circular A-71, T1, which will require agencies to implement comprehensive automated data processing system security. Although the Bureau's draft guidance mentions encryption for computer communications, it does not provide any guidance for determining when personal data transmissions warrant use of encryption techniques.

We believe that specific executive level guidance on the use of encryption for personal data transmission is needed. Several commercial firms are producing DES devices, and interest is growing among civil government agencies to use encryption techniques for data transmissions containing personal data. Some Federal agency officials told us that they felt that encryption was necessary to meet the protective provisions of the Privacy Act of 1974. However, these officials stated that their beliefs were not based on formal threat assessments made of their data telecommunications network, but rather on their perception that encryption was the best solution to prevent unauthorized disclosure within an environment in which they have no control.

The need for executive level guidance is further illustrated by the Privacy Protection Study Commission report of July 1977. The Commission was established to investigate personal data recordkeeping practices of governmental, regional, and private organizations and to recommend to the President and the Congress the extent, if any, to which the principles and requirements of the Privacy Act apply to these organizations. The Commission found that:

"* * * the Federal agency responses to the safeguarding provisions has ranged from no response at all to what may only be termed technological overkill * * *"

Therefore, a definite need should be established through a formal threat assessment, based on specific executive level guidance, before an agency uses encryption techniques for transmissions containing personal data.

Although encryption is an effective means for protecting transmissions containing classified data and highly sensitive information, it is not necessarily a cost-effective solution for protecting against privacy threats to most personal data transmissions, as indicated below.

- Although alleged wiretappings of telephone conversations have been widely publicized and some wiretappers have been convicted and penalized under law, we were unable to find a single documented case where wiretapping, authorized or unauthorized, was used specifically to intercept and exploit personal data transmissions.
- While telecommunications experts agree that a person can electronically intercept or wiretap common carrier data links, the data that may be available by electronic interception is generally unpredictable. Without the ability to address specific data, the cost of such an interception may well exceed the value of any information obtained, especially for personal data.
- The privacy threat to personal data being transmitted does not stem as much from telecommunications vulnerabilities to interception as from the potential misuse of personal information by individuals authorized access to such information in computer systems, according to knowledgeable Government officials.
- Security experts believe that encryption may leave a false sense of security, and therefore, detract from other safeguards that are essential to protect personal rights to privacy.

Also, an Office of Technology Assessment official told us that caution should be taken in implementing cryptographic techniques for telecommunications. The costs of such techniques may be prohibitive in relation to their effectiveness as a privacy safeguard.

In that regard, our previous report entitled "Computer Related Crimes in Federal Programs" (FGMSD-76-27, April 27,

1976) pointed out that most of the cases examined did not involve sophisticated attempts to use technology for fraudulent purposes, but rather they were uncomplicated acts which were made easier because management controls over the systems involved were inadequate.

Further, another of our reports entitled "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, January 17, 1977) stated that, while wiretapping and electronic interception of telecommunications were technically possible, the extent of the threat to taxpayer data from such techniques had not been established, and no known cases of unauthorized disclosure of taxpayer information traceable to use of data telecommunications had been found. Although the proposed Tax Administration System was not implemented, our report indicated that estimated costs for encrypting the data transmissions would have been several million dollars and that there was no evidence that threats to the transmission of taxpayer information warranted such costs.

In addition to being unwarranted for most personal data transmissions, the use of expensive, encryption technology is not consistent with the intent of the 1974 Privacy Act, according to the following:

--The Privacy Protection Study Commission report of July 1977 states that:

"The framers of the Privacy Act specifically intended that the safeguarding provisions not be directed toward the highly technical and exotic form of attack."

--A National Bureau of Standards publication states that procedural controls and physical safeguards produce the highest degree of protection for the lowest cost, and they satisfy the requirements of the Privacy Act. Therefore, DES should not be used by Federal agencies to safeguard personal data unless adequately justified. 1/

--NTIA officials told us that the greatest threat to privacy was the misuse of personal information by authorized users rather than third-party perpetrators. They also said solutions to privacy

1/Federal Information Processing Standards Publication (FIPS PUB) 65, 1, Aug. 1979, p. 21.

issues were achievable through administrative controls which agencies were responsible for establishing under the Privacy Act.

Therefore, it is clear that the use of DES technology for electronic transmissions is expensive and will not protect against the principal threat to personal data as intended by the 1974 Privacy Act. We agree with the officials of the National Bureau of Standards, the Office of Technology Assessment, and NTIA that encryption, including DES, is not the best solution for protecting against the primary threat to privacy--the misuse of personal data by authorized users within Federal agencies--as intended by the Congress when passing the Privacy Act. Therefore, clear executive level guidance is needed to assist agencies in determining, based upon threat assessments and risk analyses, if and when encryption is needed to protect transmissions containing personal data.

CONCLUSIONS

OMB issued policies and implementing guidelines to Federal agencies for establishing security programs for agencies' automated information systems which emphasized data processing, but generally neglected the telecommunications supporting such systems. Also, NTIA's ongoing effort to formulate telecommunications policies and guidelines does not specifically address telecommunications protection for personal data transmissions.

Under existing OMB directives, civil Government agencies are responsible for making risk analyses of the data processing portions of agencies automated information systems. While these agencies' computer security programs were initiated to comply with OMB direction, their programs emphasized the data processing portions and generally neglected telecommunications. Risk analyses should specifically include data telecommunications networks for determining that degree of protection beyond which the cost of penetrating or subverting the network becomes greater than the benefits to be gained. However, civil agencies have not made such risk analyses. We believe the principal reason for this situation is the lack of executive level direction and guidance.

While there is a growing interest among civil government agencies to use encryption for protecting their transmissions containing personal data, this technology is not necessarily a cost-effective solution for protecting against privacy threats to most personal data transmissions. We believe that use of this technology, based on intuitive judgments, is not consistent with the intent of the 1974 Privacy Act.

Therefore, we believe civil government agencies need additional executive level policy guidance on telecommunications protection. Additional guidance will assist agencies to (1) assess the impact of supporting telecommunications vulnerabilities on their data processing systems, (2) determine, through appropriate risk analyses, whether additional safeguards and controls are needed to protect personal data transmissions, and (3) determine whether encryption techniques are appropriate for such transmissions.

RECOMMENDATIONS

We recommend that the Director, Office of Management and Budget, in cooperation with the Secretary of Commerce, direct the Administrator, National Telecommunications and Information Administration, Department of Commerce, to develop clear guidance for Government data transmission protection that:

- Is consistent with the computer security guidance published by the National Bureau of Standards for automatic data processing.
- Specifically includes risk analyses of the data telecommunications networks supporting data processing systems used to maintain personal and other sensitive information.
- Includes standards and implementing guidelines for determining the appropriateness of using encryption techniques for electronic transmissions, including those containing personal information.

AGENCY COMMENTS AND OUR EVALUATIONS

GSA endorsed our recommendations, and NTIA agreed that current executive level guidance on telecommunications protection was not adequate for personal information.

OMB agreed that personal information might need protection. However, it contended that the direction and guidance in OMB Circular A-71, T1, was adequate for telecommunications.

As pointed out on page 16 of this report, under three sections of the Privacy Act Federal agencies are responsible for accurate maintenance and appropriate safeguards to records as well as the establishment of rules of conduct for persons involved in maintaining record systems. These sections imply that agencies are responsible for vulnerabilities in telecommunications networks used to support agency record systems containing personal data. On page 16 we point out that, because of the lack of executive level guidance, five agencies responding to OMB's direction and guidance had not included risk analyses of telecommunications vulnerabilities in their computer security programs and plans. Also, some agency officials felt that encryption was the only solution for protecting personal data transmissions. Therefore, we agree with NTIA that current executive level guidance on telecommunications protection is not adequate for personal information.

OMB disagreed with the statement "Federal data telecommunications networks can generally be viewed as a separate entity for purposes of assessing automated information system security." We recognize that Federal data telecommunications networks can be viewed as a separate entity only for identifying telecommunications vulnerabilities and revised this report to be consistent with this recognition.

CHAPTER 4

PRIVACY IMPACT OF

SHARED DATA TELECOMMUNICATIONS FACILITIES

AND ASSOCIATED NETWORK CONTROLS

A shared data telecommunications network can be constructed to provide equivalent or better controls for network use than provided by existing individual civil agency data telecommunications networks.

For instance, unauthorized use of telecommunications network facilities to gain access to data processing computer systems can be controlled or prevented through common-user network controls and associated procedural arrangements for use authentication, routing and community of interest controls, transmission protocols, and circuit and network use accounting.

Thus, common-user network controls can be used to allow or deny telecommunications network access to any data terminal user and to control transmissions between any data terminal and data processing computer, based on criteria separate from that used for controlling use of data processing computer resources. The use of the telecommunications network to share or exchange personal information not complying with applicable legislation can also be precluded by implementing telecommunications controls which are not directly controlled by the information users. Therefore, a potential threat to privacy--through the unauthorized exchange of information via the common-user telecommunications network--can be controlled.

During this review, we recognized that a major concern of the Congress is to maintain the integrity and confidentiality of personal information which the Government collects, distributes, and uses. Therefore, we questioned whether a civil Government shared data telecommunications network, by its very nature and existence, would encourage and increase the opportunity for abuse of privacy information beyond that which might occur with separate individual agency data telecommunications networks.

A data telecommunications network, dedicated or shared, performs one general function--to faithfully deliver electronic messages between geographically separated data terminal equipment. For the most part, both Government

dedicated and shared data telecommunications networks consist of the transmission and switching facilities which commercial carriers provide and the public shares. Also, the major threat of abuse to personal information maintained by Federal agencies is not due to the technology or type of data telecommunications network used, but rather, according to privacy experts, from misuse by individuals having authority to access and use the information.

Therefore, the privacy implications of shared versus dedicated data telecommunications networks involve (1) the potential threats to personal information during transmission and (2) the unauthorized use of the transmission network to gain access to data processing computers maintaining such information. In both cases, use of common-user transmission technology and common-user network controls can provide equal or better control over network use than those existing dedicated telecommunications networks procured separately by individual agencies, as discussed in the following sections.

COMPARISON OF DEDICATED AND SHARED NETWORK VULNERABILITIES

An important consideration for privacy is maintaining integrity of personal information. For telecommunications, data transmission integrity means the assurance that all input data are correctly received and delivered and have not been accidentally or intentionally altered or destroyed within the telecommunications environment. The telecommunications techniques used to assure data transmission integrity and their privacy implications are no different for a shared Government telecommunications network than for a dedicated Government network.

Another consideration is the vulnerability of dedicated versus shared transmission facilities to surreptitious interception. Telecommunications experts informed us that the degree of difficulty to intercept and exploit data transmissions is greater in common user links of telecommunications networks because, as the complexity of technology and sophistication for sharing and routing data circuits increases, the difficulty of interception and exploitation also increases.

COMPARISON OF SHARED VERSUS DEDICATED
NETWORK CONTROLS TO PREVENT MISUSE

Network controls of shared data telecommunications networks can provide safeguards against unauthorized use of transmission facilities to exchange personal data and provide added barriers to unauthorized users attempting to gain access to data processing systems containing such data. The unprotected dedicated networks we reviewed did not have such controls.

Also, telecommunications network controls can be provided, in addition to the data processing controls used for controlling access to a data processing system resource. These telecommunications controls can automatically (1) deny network access to users failing to provide acceptable responses to network challenges, (2) produce usage records, including incorrect or improper access attempts, and (3) permit interconnections between specifically designated data processing facilities and remote data terminals when only previously authorized. Also, a human controller can be notified when certain network controls are triggered. Thus, network controls can assist in reducing the principal potential threat to privacy--the unauthorized exchange of personal information.

Also, telecommunications network controls can provide private subnets for individual agencies within a larger shared Government data telecommunications network. Such private subnets would be no different than the dedicated networks currently in use, except that the network controls would allow or deny usage of transmission facilities.

Private subnets are already provided by certain commercial shared data telecommunications networks, commonly known as Value Added Networks, and are used by some of the civil agencies we reviewed. These networks, configured within large publicly shared telecommunications utilities, contain network features to control data transmission service and interconnections among multiple users.

Officials from two Value Added Network carriers told us that their networks, in addition to providing transmission economies, provided greater control over the use of their transmission facilities than that provided by civil agency dedicated networks.

Also, GSA's Advanced Record System (ARS), configured within a larger public network and shared by many civil agencies, had greater control over its use and user transmissions than the dedicated civil agency networks we reviewed.

The table below compares telecommunications network controls of (1) a potential shared civil Government-wide network, (2) the existing shared ARS, and (3) the dedicated civil agency networks we reviewed.

<u>Network control features</u>	<u>Potential shared network</u>	<u>Existing shared network ARS</u>	<u>Existing civil agencies dedicated network</u>
Requiring authentication to use transmission facilities	yes	yes	no
Report invalid authentications	yes	yes	no
Validate authority to interconnect with requested destinations by authorized users	yes	yes	no
Report unauthorized request	yes	yes	no
Assign unique terminal sequence number to user transmissions	yes	yes	no
Summary accounting and reporting for each interagency transmission (by sending terminal and receiving terminal)	yes	a/no	no

a/Planned in 1980 ARS' modification of message switching centers.

As the table shows, network controls for a shared communications network provide added barriers to remote users before they encounter the separate controls already in use in data processing systems. They can also detect, deny, and record unauthorized attempts to use telecommunications facilities to exchange data or to gain unauthorized access to data processing systems, including those containing personal data. Further, they can increase executive branch and congressional oversight by recording and reporting statistics on electronic data transmissions among and between agencies using shared data telecommunications networks.

CONCLUSIONS

On the basis of the above, we believe that a properly designed civil Government shared data telecommunications network, with appropriate network controls, will increase the difficulty of unauthorized network use to gain access to civil agency data processing systems containing personal information. We also believe that such controls will discourage, rather than encourage, unauthorized electronic exchanges of such information. In addition, we believe that our previous reviews on data processing showed that Federal and other authorized user controls for collecting and handling personal information should be strengthened to increase privacy protection for personal and other sensitive information, regardless of whether shared transmission facilities and related network controls are used. Further, we believe that, although network controls cause some user inconvenience, such controls to strengthen existing privacy protection safeguards should be favored over user inconvenience.

As pointed out in chapter 3 of this report, Federal agencies are responsible if certain provisions of the 1974 Privacy Act are violated as the result of telecommunications network vulnerabilities. Therefore, to consider approval of a common-user data telecommunications network for civil Government agencies, the Congress should be provided engineering analyses of selected architectures, including the comparative privacy and security strengths and weaknesses of these architectures, as well as those of the dedicated networks currently in use. Such analyses should be included as part of the comprehensive study recommended in chapter 5 of this report.

AGENCY COMMENTS AND OUR EVALUATION

GSA generally endorsed our recommendations. GSA informed us it had completed a data telecommunications study for OMB in July 1980 which addressed common-user, shared resource, and dedicated resource networks, including their privacy implications. This study generally supports our conclusions. Specifically, the GSA report states that:

- The characteristics of alternate routing of data in a common-user system flowing between two end points provide an inherent degree of security to a user, since the system increases the difficulty in intercepting or altering data by an outside source, or decreases the opportunity to gain access to all the data by a particular user.
- The common-user system offers the same inherent features for privacy as for the above-mentioned security characteristics.
- Due to the shared resources, a high measure of privacy and security can be designed into the system and maintained by centralized management control.

NTIA also acknowledged that a consolidated, common-user network would be more able to support network controls and their attendant security overhead than a discrete individual system. However, NTIA cautioned that similar arguments made in support of the proposed National Data Center did not remove congressional fears that aggregation of sensitive personal information represented a tempting object for manipulation.

We recognize and share congressional concerns about the aggregation of sensitive information in shared data files and weaknesses in data processing controls. Many of our previous reports on agencies data processing activities have demonstrated our concern. However, this report addresses shared use of transmission facilities, not shared use of data processing facilities and data files. As pointed out on page 29 of this report, the controls over use of shared transmission facilities, such as those used by commercial Value Added Network carrier companies, are in addition to any safeguards and controls agencies have implemented for their data processing resources and cannot, except through collusion, be manipulated by using agencies. These common-user network controls can provide an independent mechanism,

not used with dedicated networks, for reporting interconnections made and the volume of transmissions exchanged between agencies using the network.

OMB questioned whether a common-user network could provide better protection of sensitive information than a dedicated network. The Departments of the Interior and Agriculture and the Association of Data Processing Service Organization had similar comments. However, OMB said it was not convinced that the transmission of personal data represented a significant threat to personal privacy.

We agree that the major threat of abuse to personal information maintained in Federal automated information systems is not due to the technology or type of data telecommunications network an agency uses. We recognize that a common-user network can only provide equal or better controls for privacy protection of data transmissions. Therefore, we have amended this report to be consistent with that recognition.

The purpose of this chapter is not to suggest that the Government should implement a common-user data telecommunications network to provide better privacy protection for personal data transmissions. Rather, we have tried to show that the privacy implications of such transmissions should not be a deterrent from achieving potential economies by implementing a common-user data telecommunications network.

CHAPTER 5

SHARED DATA TELECOMMUNICATIONS NETWORK--

A POTENTIAL FOR SIGNIFICANT SAVINGS

The Government can achieve significant savings by using a shared data telecommunications network instead of continuing to use certain dedicated Government networks. Dedicated networks were procured to support separate and single agency data processing systems. Using available common-user transmission technology, shared telecommunications facilities can result in significantly greater economies while providing equivalent or better controls for privacy protection of data transmissions, as discussed in chapter 4. The costs of data telecommunications for the civil Government were not readily identifiable, but estimates of annual costs ranged from \$100 million to \$200 million, with an annual growth rate of 10 to 25 percent.

Certain civil departments and agencies have achieved some savings by integrating telecommunications requirements and sharing data transmission services. Also, the Department of Defense and the private sector have achieved savings from similar actions. On the basis of savings which have been achieved and the potential savings which various studies of departmentwide shared networks have indicated, we believe that use of a shared network for civil Government telecommunications requirements can significantly reduce total Federal data telecommunications costs. These savings are in addition to those which have been achieved through sharing on a unilateral department or agency basis. Past experience with consolidation of telecommunication resources indicates a potential savings of at least 20 percent.

However, before proceeding to implement a shared data transmission system, the executive branch should clearly identify both the monetary benefits of such a system and its implications on the integrity and confidentiality of personal data to the Congress.

PROLIFERATION OF DEDICATED NETWORKS

The most rapidly growing area of Federal telecommunications is in data telecommunications. This growth is not taking place in a coordinated cost-effective manner. Separately acquired data telecommunications networks are being procured from the same commercial common carriers to cover identical locations with increasing duplicative and overlapping transmission paths and facilities.

This is the result of separate agency planning, acquisition, and implementation without the benefit of an established civil Government plan to coordinate requirements and provide services. Generally, these separately acquired networks do not include telecommunications network features for controlling unauthorized connections and use of network facilities.

GSA is responsible for acquiring and managing general-purpose telecommunications for civil Government agencies. But GSA has not provided civil agencies an effective alternative for their dedicated data telecommunications networks as it has for shared voice communications with the Federal Telephone System. This contributes directly to the proliferation of dedicated data telecommunications networks.

In 1960 GSA made a study to determine the feasibility of integrating all existing voice and data telecommunications systems within the civil Government. The study, in which 53 departments and agencies participated, showed that it was feasible to establish a unified Federal Telecommunications System (FTS).

As envisioned, FTS would provide for telephone, teletypewriter, facsimile, and data services for both peacetime and emergency use with automatic switching. The record portion of FTS, called ARS, basically provides slow speed data transmission capabilities.

The proliferation of dedicated data telecommunications networks by civil Government agencies has been caused, in part, by the inability of ARS to meet the evolving high-speed data transmission needs in the civil Government. ARS was originally designed as a teletypewriter system and was not improved for rapid response and high-speed computer related data transmissions with modern technology. Therefore, ARS has limited capacity and has become saturated through increased use by the Veterans Administration and the Social Security Administration. Therefore, it was not available to all civil government agencies. Further, GSA reduced its planning activities for improving ARS or for providing additional Federal common-user data telecommunications services as a result of congressional objections.

In that respect, the President's Telecommunications Reorganizations task force report stated, in part, that because of civil agencies disenchantment with ARS and congressional restrictions placed on GSA which precluded it from replacing ARS with a modern shared data transmission capability, dedicated data telecommunications networks have proliferated in the Federal Government.

Since ARS cannot meet modern data telecommunications requirements, many civil agencies are using the FTS telephone segment for data transmission. However, since the FTS telephone segment was designed for voice transmission, it is not the best technical and economical approach for many civil agencies' modern data telecommunications needs. Also, because FTS does not have designed security features, FTS dial-up lines are generally open for use to interconnect data terminals and facilities anywhere in the United States without authenticating user authority to gain access to the network.

The map on page 37 shows the geographical coverage of only three dedicated networks and illustrates the duplication of transmission paths and facilities. While this map is limited to networks in three agencies at least 31 dedicated networks have wide geographic coverage, as listed below:

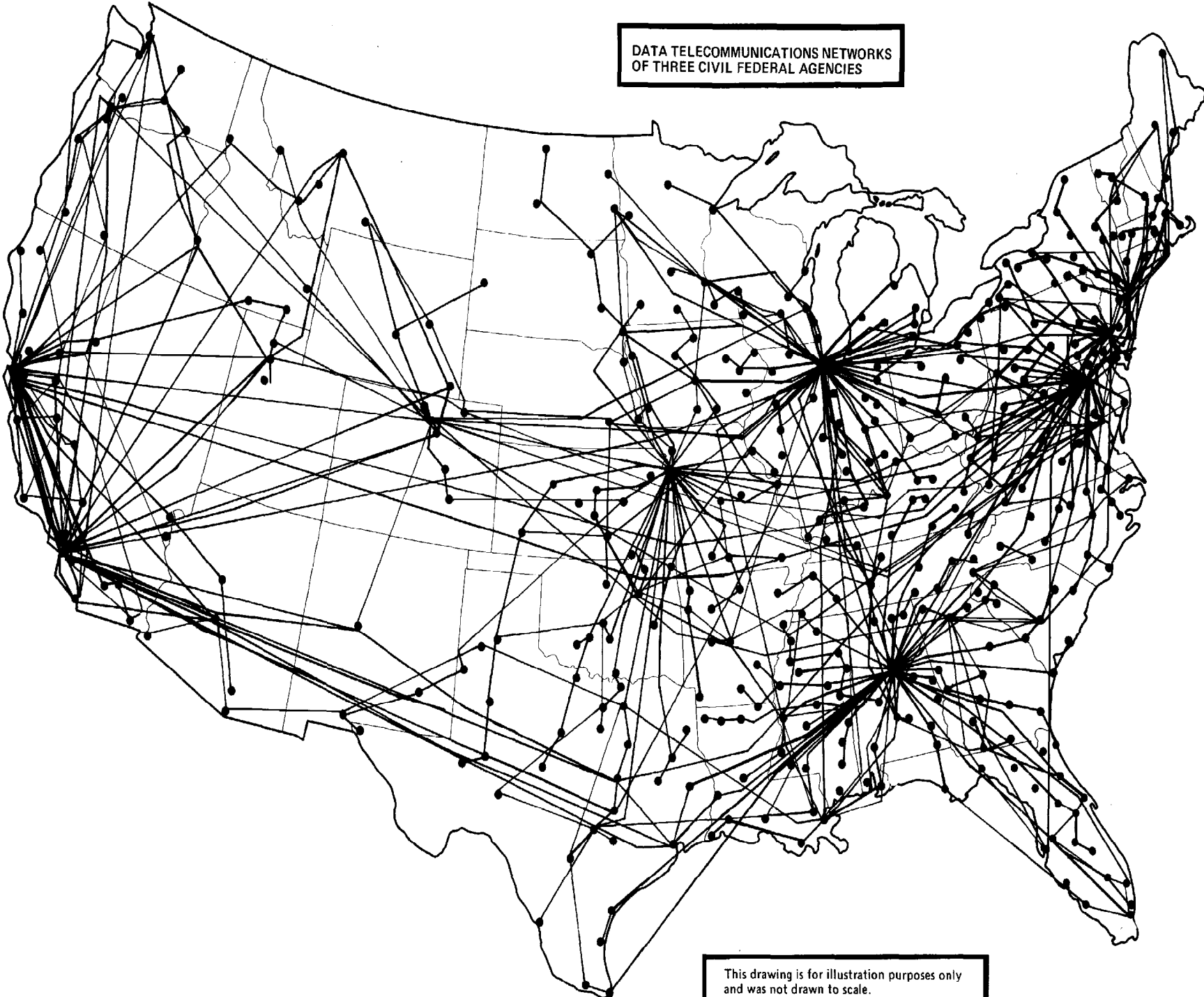
<u>Department/agency</u>	<u>Number of major networks</u>
Agriculture	4
Commerce	7
Energy	2
Health and Human Services	4
Interior	2
Justice	7
Treasury	4
Veterans Administration	<u>1</u>
Total	<u>31</u>

In addition to these networks, civil agencies also operate several small networks which are not in this list. If all agency networks were drawn on a map, the interconnecting lines would not be distinguishable.

ECONOMICAL POTENTIAL OF SHARING

During our review we did not attempt to determine the specific economic advantages of using a civil Government shared data telecommunications network compared to using separate civil agency dedicated networks. However, we did confirm that savings were achieved by certain agencies through circuit sharing. Also, we evaluated Government sponsored studies for three agencies which concluded that

DATA TELECOMMUNICATIONS NETWORKS
OF THREE CIVIL FEDERAL AGENCIES



This drawing is for illustration purposes only
and was not drawn to scale.



data transmission costs could be significantly reduced by integrating and sharing agency data telecommunications resources. The chart below provides examples of actual and potential savings through shared arrangements within the civil Government.

<u>Agency</u>	<u>Savings</u>		<u>Percent of cost reduction</u>
	<u>Achieved</u>	<u>Projected</u>	
Bureau of Reclamation, Dept. of the Interior	\$400,000 annually		53
U.S. Customs Service, Dept. of the Treasury	\$600,000 annually		49
Federal Bureau of Investigation	\$156,000 annually		24.5
Social Security Administration		\$16 million in 5 years	23
Department of Agriculture		\$20-45 million in 8-1/2 years	27-43
Department of Justice (less the Federal Bureau of Investigation)		\$2 million in 6 years	15

Bureau of Reclamation

The Bureau of Reclamation, Department of the Interior, has a large data telecommunications network consisting of 22,000 miles of circuitry serving seven bureaus within the Department, seven other Federal agencies, and six non-Government organizations. The network connects over 700 terminals located in 70 different cities, with the Bureau's computer center in Denver, Colorado. About 500 of the terminals on the network are shared circuits. We estimated this system reduced costs by \$400,000 a year and eliminated the need for 85,000 miles of circuitry. This estimated savings represents a 53-percent cost reduction when compared to a nonshared system providing equal service capability.

U. S. Customs Service

Customs has an extensive data telecommunications network serving 1,200 terminals located at ports-of-entry, international airports, and selected preclearance facilities in Canada, Bermuda, and the Bahamas. Although about 700 circuits in this network were shared, Customs officials, concerned with increasing costs for data transmission, installed

more sophisticated devices to increase further circuit sharing and reduced their transmission costs an additional \$600,000 a year.

Federal Bureau of Investigation

The Bureau recently installed 20 leased devices to permit sharing on selected high-speed circuits to the National Crime Information Center by major State and city law enforcement agencies. By installing the circuit sharing devices on commercial telecommunications vendor premises, the Bureau decreased the network mileage by 35,302 miles and reduced communications costs by about \$156,000 a year. This estimated savings represents 24.5 percent of the Bureau's cost for high-speed service.

Social Security Administration

A study sponsored by NTIA showed that Government costs could be potentially reduced by about \$16 million over a 5-year period if the Social Security Administration used a data telecommunications network which could be shared by other civil Government agencies rather than implementing its own dedicated network.

Department of Agriculture

A detailed requirements and economic study identified the most cost-effective transmission network configuration to satisfy the domestic data telecommunications requirements for the Department of Agriculture over the next 7 to 10 years as a common-user data telecommunications network. This study compared costs for continuing separate dedicated bureau networks with costs for a departmentwide integrated data telecommunications network. This study showed that Agriculture could obtain present value savings from \$20 million to \$45 million over an 8-1/2 year period if a common-user data telecommunications network was implemented. The study also showed that additional savings would be achieved if the system's life was extended beyond 8-1/2 years.

Department of Justice

A similar study projected that an integrated data telecommunications network would reduce the data transmission cost for the Department by at least \$330,000 annually, when compared to the cost for continued use of its dedicated networks. The Federal Bureau of Investigation was not included in this study.

Economic potential of sharing
should be verified

The above studies show that significant savings are possible by integrating small dedicated networks into larger shared systems. We believe that a similar study, which will include all civil agencies, will show that there is a potential for comparable savings if (1) the proposed shared systems are integrated further or (2) a properly designed civil Government data telecommunications network is implemented for shared use in such areas and for such agencies as would be reasonable and effective.

Therefore, we believe that a study to determine the savings that can be achieved under various alternative design concepts should be made. GSA has legislative authority and responsibility for economies and efficiency of general-purpose telecommunications for the civil Government. ^{1/} We believe that GSA is currently the appropriate agency to make or sponsor such a study, but it needs the cooperation of and participation of NTIA.

According to GSA officials, they are reluctant to perform such a study because of the restrictive language inserted annually in their appropriations act which states:

"None of the funds available under this act or under Section III of the Federal Property and Administrative Services Act of 1949 shall be obligated or expended for the procurement by purchase, lease or any other arrangement, in whole or in part, of any or all the automatic data processing system, data communications network, or related software and services for the joint General Services Administration-Department of Agriculture MCS project 97-72 contained in the Request for Proposal CDPA 74-14, any successor to such a project, or any other common user shared facilities authorized under section III of the Federal Property and Administrative Services Act of 1949."

^{1/}Section 201 of the Federal Property and Administrative Services Act of 1949, as amended, and section F of the act of June 14, 1946, together give GSA apparent authority to regulate, procure, and operate general-purpose telecommunications services for certain executive agencies.

As we interpret that language, GSA can fulfill its responsibility for telecommunications planning, including studies and analyses, but is prohibited from using funds to implement any new common-user data telecommunications networks without congressional approval.

In a June 26, 1980, letter, the Chairman, House Committee on Government Operations, pointed out to the Chairman, House Committee on Appropriations, Subcommittee on Treasury, Postal Service, General Government, that the restrictive language in GSA's appropriations bill for fiscal year 1981 may be counterproductive and contrary to the resource sharing provisions of Public Law 89-306 and the Paperwork Reduction Act of 1980 (H.R. 6410). The Chairman also stated that the situation which placed the appropriations restrictions on GSA in 1974 no longer existed. We agree with this position.

If the executive branch questions GSA's authority to make a comprehensive study it should seek clarification from the appropriate congressional oversight committees before directing GSA to make such a study for determining the most cost-effective method of meeting total civil Government telecommunications requirements. We also believe that the executive branch should present these oversight committees with its plans for making such a study, including the time and resources required.

For the Congress to knowledgeably consider the merits and problems of proceeding with a shared civil Government data telecommunications network instead of continuing with separate dedicated networks for individual agencies, it needs complete and accurate facts. Therefore, the comprehensive study should include (1) the levels of savings achievable, (2) the provisions for privacy protection, (3) the implications on the telecommunications industry and Federal policies for proposed management arrangements for types of procurement (services versus facilities) and ownership (lease versus purchase), and (4) the impact on the affected civil agencies' data telecommunications costs and operations.

Concerning implications on industry and Federal policies, specifically involving competition, NTIA should participate in these aspects of the study because of its responsibilities for formulating and coordinating policy for Federal telecommunications.

CONCLUSIONS

This review has shown that the rapid growth in data telecommunications in the civil Government has been uncoordinated and without strong executive level management. Costly, duplicative, and overlapping dedicated civil agency data telecommunications networks continue to proliferate, although a shared civil Government network is operationally and technically feasible. Also, it appears that such a network can provide significant savings and increase reliability of service for agencies not having unique transmission requirements.

Some agencies have reduced their data transmission costs through sharing arrangements. However, we believe these actions are piecemeal approaches and should be expanded by strong central direction and uniform coordination for all civil agencies.

Although GSA has legislative authority and responsibility for providing economic and efficient general-purpose telecommunications for the civil Government, it has not made a comprehensive study of total civil Government data telecommunications requirements and the best methods of satisfying those requirements. GSA has not made such a study because it has interpreted the restrictive language placed annually in its appropriations acts as preventing it from implementing new common-user networks. We believe that the executive branch should seek clarification from the appropriate congressional oversight committees and present these committees with its plans for making such a study, including the time and resources required.

We concur with the requirement for prior congressional approval before GSA uses funds to implement any new common-user data telecommunications network for the civil Government. To do this, the Congress needs complete and accurate information. The information should include preliminary network design, with cost benefit analyses, and provisions for privacy, competition, management controls, and the impact on the affected civil agencies.

RECOMMENDATIONS

We recommend that the Director, OMB, take appropriate action, including seeking concurrence from appropriate congressional oversight committees, to have GSA make or sponsor

a study which will clearly identify the merits and problems of proceeding with a shared civil Government data telecommunications network instead of continuing with separate dedicated networks in such areas and for such agencies as would be reasonable and effective.

In fulfilling that task, OMB, with the assistance of the Administrators of General Services and the National Telecommunications and Information, should provide to the appropriate oversight committees complete and accurate information on a potential shared data telecommunications network for civil Government agencies. This information should include

- a preliminary network design with levels of economy achievable;
- provisions for privacy protection;
- implications on industry and Federal policies for types of procurement, ownership, and management controls proposed; and
- the impact on the affected civil agencies' data telecommunications costs and operations.

The Congress should limit the development and implementation of new separate dedicated data telecommunications networks pending completion of the study and congressional determination on whether to proceed with a shared civil Government data telecommunications network.

AGENCY COMMENTS AND OUR EVALUATION

OMB, NTIA, and the Department of Agriculture agreed that certain benefits might be associated with the establishment of a shared civil data network. However, they said our report did not address all the pros and cons for a common-user network. Generally, they stated our conclusion about economies of a common-user network could only be drawn after a comprehensive study was completed.

We recognize that a comprehensive study to address all factors for and against implementing a common-user network is needed. We believe our report provides sufficient evidence of potential savings to justify such a study.

GSA endorsed the recommendations of this report and had already initiated actions consistent with our recommendations. The Administrator of General Services notified GSA's congressional oversight committees that it had made a data telecommunications feasibility study requested by OMB. That study was completed in July 1980 and showed that, although certain agency requirements might not be accommodated, a common-user network or a shared data telecommunications utility was the primary candidates to satisfy a large number of agency requirements, with increased performance and lower cost.

Agriculture also stated that the report over emphasized the Government's designing, constructing, implementing, and operating its own network. We do not intend to suggest Government ownership over commercial service. We, therefore, recommend that a comprehensive study be made which includes evaluating the effects on the telecommunications industry and proposed management arrangements for types of procurement and ownership.

Justice stated that certain mission-oriented data transmission requirements could not be adequately supported by a common-user network, such as ARS. We recognize that such a network will not satisfy all unique transmission requirements of certain agencies and have revised our conclusions to be consistent with this recognition.

The U.S. Independent Telephone Association also felt that a comprehensive study addressing the points we recommended would provide valuable planning information. However, the Association of Data Processing Service Organization stated that a separate study would be required for commercial teleprocessing services which would be integrated into telecommunications networks, and it questioned how free and open competition in the procurement process would be assured if a single network was recommended.

We do not believe that a separate study would be required for commercial teleprocessing services because requirements for data telecommunications between Government agencies and commercial data processing companies should be included with other data telecommunications requirements in a single comprehensive study. We also recommend that the implications of a common-user network on competition and the telecommunications industry should be considered in the comprehensive study.

RICHARDSON PREYER, N.C., CHAIRMAN
 ROBERT F. DRINAN, MASS.
 GLENN ENGLISH, OKLA.
 DAVID W. EVANS, IND.
 PETER H. ROSENBERG, PA.
 TED WEISS, N.Y.

THOMAS B. KIRKNETT, OHIO
 M. CALDWELL BUTLER, VA.
 JOHN H. ENLEBORN, N.J.
 225-3741

NINETY-SIXTH CONGRESS
Congress of the United States
House of Representatives
 GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS
 SUBCOMMITTEE
 OF THE
 COMMITTEE ON GOVERNMENT OPERATIONS
 RAYBURN HOUSE OFFICE BUILDING, ROOM B-349-B-C
 WASHINGTON, D.C. 20515

August 10, 1979

Honorable Elmer B. Staats
 Comptroller General
 U.S. General Accounting Office
 441 G Street, N.W.
 Washington, D.C. 20548

Dear Mr. Staats:

In connection with its legislative and oversight responsibilities for the Privacy Act of 1974, this subcommittee has had a longstanding interest in the adequacy of technical and administrative safeguards employed by agencies in their computer and telecommunication systems.

Earlier this year, GAO issued a report noting serious deficiencies in the computer security programs of most federal agencies. The report did, however, anticipate progress in this area with the issuance of new guidance by OMB and with action by individual agencies. In spite of any improvements in computer security, it appears that the threat of indiscriminate or improper use of government-held information may be exacerbated through the interconnection of data sources through high-speed, high-volume telecommunication systems.

At the same time, I understand that there may be dollar savings in establishing a more sophisticated government common user telecommunications system. Before proceeding with such a system, it is important that we clearly identify not only the monetary benefits of such a system but also its implications for privacy, security, and the exchange of information between government agencies.

I request that GAO undertake a study to assess the impact of new telecommunications technology on government information practices. As part of this study, you should determine the extent of information exchange within and between agencies, and estimate how the scope or volume of data exchange would be affected by new technology. Also, you should compare the adequacy of privacy and security safeguards for the existing network with the capability of alternative systems.


Your study of common-user telecommunication systems should also address the following questions:

Honorable Elmer B. Staats
August 10, 1979

- Will an advanced telecommunication network, by its very nature and existence, encourage and provide the means for privacy information abuse beyond those abuses which might occur through "open-market" procured data telecommunication services?
- What kind of procurement, ownership, and management controls are needed to protect information carried by a common-user data telecommunication system?
- Is such a system, in fact, less expensive or more efficient than individually procured, free market place subsystems?
- What would be the costs of additional privacy management, for specialized administrative privacy controls, and for technical system privacy constraints?

Any questions concerning this study should be addressed to Timothy H. Ingram, subcommittee staff director. Mr. Ingram can be reached at 225-3741.

Cordially,


Richardson Preyer
Chairman

EDWARD M. KENNEDY, MASS., CHAIR

BIRCH BAYH, IND.
ROBERT C. BYRD, W. VA.
JOSEPH R. BIDEN, JR., DEL.
JOHN C. CULVER, IOWA
HOWARD M. METZENBAUM, OHIO
DENNIS DE CONCINI, ARIZ.
PATRICK J. LEAHY, VT.
MAX BAUCUS, MONT.
HOWELL HEFLIN, ALA.

STROM THURMOND, S.C.
CHARLES MCC. MATHIAS, JR., MD.
PAUL LAXALT, NEV.
ORRIN G. HATCH, UTAH
ROBERT DOLE, KANS.
THAD COCHRAN, MISS.
ALAN K. SIMPSON, WYO.

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, D.C. 20510

DAVID ROES
CHIEF COUNSEL AND STAFF DIRECTOR

August 15, 1979

Honorable Elmer B. Staats
Comptroller General
General Accounting Office
Washington, D. C. 20548

00-00000000

Dear Mr. Staats:

I am concerned about a growing threat to privacy posed by personal information in digital data transferred about the country over telecommunications networks by Federal civil agencies. We are witnessing proliferation of data banks containing billions of records detailing private lives of citizens. When these collections are coupled with capacity to transmit data records at high speed between agencies, there emerges a potential for a de facto national data bank whose files, though physically distributed about the country, can become one unified file through technological gathering capacity.

I ask that the General Accounting Office examine, review and analyze existing and alternative data telecommunications services, systems configurations, management structures and controls on data transmission from and between Federal civil agencies.

The prime objective is to ensure that private information about citizens gathered or yielded in trust by them shall not be used or made vulnerable to use beyond lawful purpose of collection or beyond citizen understanding of intended use.

GAO's inquiry should examine access controls on telecommunications services through which personal data may be transmitted. Please look into cases of unauthorized data disclosure or utilization by agency employees otherwise having authorized access to files. My concern ultimately envisions legislation providing protection of information, in part through controls on data telecommunications systems. This will tend to diminish abuses caused by indiscriminate interagency data sharing, machine searching, matching, and correlation.

Complete analyses of telecommunications data and privacy must be done, part-and-parcel, with those of data processing, system files bank, and privacy protection. Many studies exist, however, in the latter. GAO's emphasis, therefore, should be on data telecommunications systems -- their management and privacy controls.

Honorable Elmer B. Staats
August 15, 1979

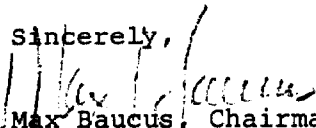
As a secondary issue, please have the analysis encompass the issue of protection from disclosure of personal information and sensitive but unclassified information to unauthorized persons attempting to intercept telecommunications data or to penetrate data banks using telecommunications circuits.

Specifically, I ask that GAO answer the following questions:

1. What is the present level and kind of abuse of privacy information involving use of existing data telecommunications networks?
2. What are the present management and technical privacy controls for use of these circuits?
3. What is the assessment of adequacy of these controls?
4. Maintaining current data telecommunications network configurations and procurement practices, what system management privacy controls and technical access constraints are needed to protect privacy information at least to Privacy Act levels?
5. Will a government-wide, common-user data telecommunications network necessarily, of itself, increase abuse or provide enhanced opportunity for abuse of privacy information?
6. What additional data telecommunications system management privacy controls and technical access constraints would be needed to protect privacy information at least to the Privacy Act requirement levels, should a government-wide, common-user network be developed?
7. What, if any, are significant economies to be achieved by developing a government-wide, common-user data telecommunications network?
8. What additional data telecommunications system legislation does GAO suggest may be needed for protection of privacy information?

Thank you for your prompt inquiry into these issues.

Sincerely,


Max Baucus, Chairman
Subcommittee on Limitations of
Contracted and Delegated Authority



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

AUG - 7 1980

Mr. William J. Anderson
Director
General Accounting Office
Washington, D.C. 20548

Dear Mr. Anderson:

In response to your request of June 20, 1980, we are providing comments on the draft report entitled "A Federal Civil Agency Common-User Data Telecommunications Network - A Potential for Economies and Improved Data Protection" Code 941159 (CIM-80-17). This report addresses two important questions: the benefits of common-user data telecommunications networks and the protection of Federal data telecommunications networks. Unfortunately, the draft report combines these issues in a fashion which is both confusing and raises spurious policy issues. In our comments we have attempted to separate the various issues and address them individually.

The report asserts that there may be certain economies realized through greater use of common user data networks. In order to document these economies, and answer a number of related policy questions, the report recommends that OMB initiate a study to "clearly identify the merits of proceeding with a shared civil government data telecommunications network."

We agree with the GAO that there may be certain benefits associated with the establishment of a shared civil data network. Earlier this year we tasked the General Services Administration to develop an issue paper which would address the pros and cons of such a network versus continuing dedicated agency networks. Our goal is to develop a long-term policy for meeting the data telecommunications needs of civil agencies in the most economic and efficient manner possible. The draft GAO report does not offer substantive information that will assist us in our consideration of this issue.

The second issue is whether a shared data telecommunications network can provide a level of protection commensurate with the sensitivity of the data that will be transmitted. This issue includes the protection of national security, proprietary and similar sensitive data, as well as the protection of personal information. These types of data are related, yet distinct. Unfortunately, the report tends to lump them together and thereby create confusion.

The report suggests that a common-user network can provide better protection of sensitive information than a dedicated network. However, the only supporting evidence provided in the report is the assertion that "telecommunications experts informed us that the degree of difficulty to intercept and exploit data transmissions is greater in the common-user portion of telecommunications networks..." Whether or not a common-user network can provide better protection of sensitive information than a dedicated network appears to us to be an important, but as yet unresolved, question.

In addition to these basic issues, the report develops several other points with which we disagree. The report notes that "Federal data telecommunications networks can generally be viewed as a separate entity for purposes of assessing automated information system security." We fundamentally disagree with this statement. We believe that information, whether automated or not, should be managed on a system basis from data collection to final disposition. The system manager or user is responsible for the integrity, the utility, the protection and the management of the information in that system. To isolate one element in the system and treat it differently is to distort management's perspective of that system and thereby reduce both responsibility and accountability.

The report contends that additional OMB policy guidance is needed for telecommunications security. However, no convincing evidence of this need is presented. Policy for telecommunications security is already stated in OMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems." That policy was issued in July 1978, to ensure that Federal automated systems are adequately protected. It establishes that the head of each agency is responsible for assuring an adequate level of security for all agency data, whether processed in-house or commercially. In carrying out this policy, each agency head must assess the risk associated with the loss or misuse of agency data which is of a personal, proprietary or other sensitive nature and establish a level of safeguards commensurate with that risk. The intent of this policy is that the vulnerability of the total system - from data entry to disposition - shall be assessed. Although the transmission of data is not explicitly discussed in the policy, it is clear that this part of the system is to be included. For example, the background section discusses the "increasing use of computer and communications technology..." Similarly, each agency head is clearly assigned responsibility to establish "physical, administrative and technical safeguards required to adequately protect personal, proprietary and other sensitive data... as well as national security data." This responsibility clearly does not exclude the transmission of data. Finally, the GSA

is tasked to "assure that computer equipment, software... telecommunications services and any other related services procured by GSA meet the security requirements established by the user agency." It is clear that OMB Circular No. A-71 includes policy for the security of telecommunications networks.

In addition to this policy, a number of other initiatives are underway to improve the security of Federal automated information systems. As the draft report acknowledges, the National Bureau of Standards and National Telecommunications and Information Administration are developing policies, standards, and guidelines to assist agencies in protecting their automated data. There are also a number of classified activities underway. We find no indication in the draft GAO report to suggest that these efforts are either inappropriate or misdirected. Rather, the report seems to suggest only that there is a need for specific guidance to protect the transmission of personal information.

We agree that personal information is often sensitive and may need to be protected. However, we are not convinced that the transmission of personal data represents a significant threat to personal privacy. The draft report does not present a single documented case where personal privacy has been violated through the interception of transmissions. Furthermore, if someone was interested in illegally accessing personal data, it is unlikely that he would do so by passively intercepting data transmissions. It is much more likely he would actively seek access to the data base. The prevention of such access is clearly within the scope of responsibilities assigned by OMB Circular No. A-71.

Caution must be exercised in considering the privacy issue. It is our understanding that the GAO is discussing only the security of shared transmissions, not the security and integrity of shared data. The latter issue is much more complex and involves public policy questions regarding the integrity and desirability of shared information. Unfortunately, including references to systems such as FEDNET, TAS and NCIC, some of which do involve shared information, cloud the intended scope of the GAO report.

The draft report would have the reader believe that there are no disadvantages to common-user networks. We believe that is misleading. For example, common-user networks require that a management structure exist to manage such systems. Similarly, common-user networks remove from an agency head who manages an automated information system the responsibility and accountability for managing those resources associated with the transmission of information.

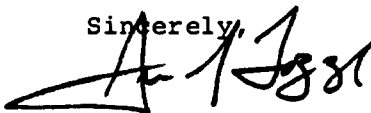
Finally, it is extremely difficult to accurately allocate user costs for the backbone provided by a common-user network. At a minimum, it requires a complex accounting system.

The report recommends that the 1968 Crime Control Act be amended to conform with the capabilities of new technologies for the interception of transmission. Such an amendment may or may not be appropriate. However, it would seem more appropriate to incorporate such a provision in legislation currently being considered by Congress (S.240) to address the illegal use of automated information. The executive branch has supported this legislation and would urge the GAO to review it for applicability to the issues being discussed in the report.

Finally, it was extremely difficult to review this report due to the lack of definitions. A number of words and phrases are used interchangeably when, in fact, they have different connotations. "Network" and "automated information system" are used interchangeably in the report. Similarly, "personal and other sensitive data" is not the same as "personal and other proprietary data." It is also not clear if it is intended that national security and similar data is to be included in these phrases. We believe that a definition section would help.

We appreciate having this opportunity to comment on the draft report. However, in light of the minimal additional information provided by the report and the questionable assumptions used in developing its recommendations, we believe that a substantial restructuring of the text would be essential before the report is released in final form.

Sincerely,



Jim J. Tozzi
Assistant Director for
Regulatory and Information Policy



General
Services
Administration Washington, DC 20405

JUL 22 1980

Honorable Elmer B. Staats
Comptroller General
United States General Accounting Office
Washington, DC 20548

Dear Mr. Staats:

This is in response to your June 20, 1980, letter, in which you requested comments on a draft audit report entitled "A Federal Civil Agency Common-User Data Telecommunications Network -- A Potential For Economies And Improved Data Protection." In general, I endorse the recommendations of the report.

You should be aware that members of the Automated Data and Telecommunications Service (ADTS) of this Agency have been working with the National Telecommunications and Information Administration (NTIA) on a related data communications study requested by the Office of Management and Budget (OMB). The request was made in a February 22, 1980, allowance letter to the General Services Administration (GSA) which is enclosed. The effort we are developing for OMB will specifically address the four points identified in the recommendations of your draft report that pertain to economics, privacy, policy, and impact of shared data communications. It will also recommend a comprehensive follow-on study of the sharing of Federal data communication systems as you had similarly proposed in your draft report.

Since your report recommends congressional notifications, you should also be aware that on May 16, 1980, I notified GSA's Congressional Appropriations Committees, as well as the House Government Operations Committee that we have embarked on the study requested by OMB. A copy of one of these three (identical) letters is also enclosed. I made these notifications because we want it to be clearly understood that we are acting in response to a specific request from OMB and in full cooperation with Congress.

We look forward to the final publication of your report as we study the best ways to address the data communications needs of the Government.

Sincerely,



R. G. Freeman III
Administrator

Enclosures



UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

AUG 8 1980

Mr. Henry Eschwege
Director, Community and Economic
Development Division
U. S. General Accounting Office
Washington, D. C. 20548

Dear Mr. Eschwege:

This is in reply to your letter of June 20, 1980 requesting comments on the draft report entitled "A Federal Civil Agency Common-User Data Telecommunications Network -- A Potential for Economic and Improved Data Protection."

We have reviewed the enclosed comments of the National Telecommunications and Information Administration and believe they are responsive to the matters discussed in the report.

Sincerely,

Mary P. Bass
Inspector General

Enclosure



UNITED STATES DEPARTMENT OF COMMERCE
National Telecommunications and
Information Administration
Washington, D.C. 20230

AUG 5 1980

Mr. Henry Eschwege
Director, Community and Economic
Development Division
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Eschwege:

Many very timely and important issues are discussed in the General Accounting Office's (GAO's) draft proposed report, "A Federal Civil Agency Common-User Data Telecommunications Network--A Potential for Economics and Improved Data Protection." The Department of Commerce shares GAO's concerns about the protection of personal privacy in an environment increasingly characterized by automated information systems. Yet, as valid as these concerns obviously are, it is easy--as Chapter 3 of the report points out--to overreact in inappropriate directions. Activity for its own sake is no solution to the critical problems discussed in the report.

We strongly support GAO's view that the deficiencies of current wiretap law suggest the need for legislative changes. In today's increasingly data-oriented environment, it makes little sense to protect voice communications while leaving other equally intimate forms of communication vulnerable to legal interception. However, GAO must do more than just recommend a specific change. Several similar proposals which were advanced in recent years met with strong opposition, primarily from the intelligence and law enforcement community. We believe that GAO's recommended change--which we strongly support--would have a much greater chance of acceptance if the report were to address directly the variety of objections which the intelligence and law enforcement agencies have voiced relating to this topic.

As we mentioned at the outset, there is little question about the inadequacy of current guidance to agencies about protection of personal information. Enclosed are more detailed comments relating specifically to the Department of Commerce's role under PD/NSC-24. As Chapter 3 points out, fitting a security (encryption) "solution" to a privacy (personal data) "problem"

doesn't necessarily improve the situation... and it may cost a lot of (taxpayer) money in the process. Clearly, as the report states, some sort of indepth risk management analysis is necessary. What is not clear, however, is how GAO would suggest that this function be institutionalized within the agencies. The impact of this recommendation would be strengthened by the addition of suggestions on the roles of user agencies as compared with central, intelligence-related agencies in carrying out this function.

GAO's argument (Chapter 4) that privacy can be enhanced in a shared system as compared with that available through adoption of discrete approaches strongly resembles arguments made in support of the National Data Center. Now, as then, there is a certain truth to the notion that a consolidated, common user system is more able to support a substantial security overhead than can discrete, individual systems. However, as discussed above, these security measures might not go to the heart of the real privacy problems. Moreover, this argument, in the case of the National Data Center, was insufficient to overcome Congress' fear that such a functional and/or physical aggregation of sensitive personal information would represent a much too tempting object for manipulation by agencies, despite the imposition of strong security measures. We see little to indicate any change of heart in this area by Congress.

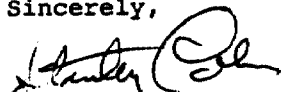
GAO's arguments about the economic efficiency of shared systems (Chapter 5) follow a theme increasingly common to recent GAO reports, favoring increased consolidation of telecommunications services and facilities. We find no new arguments are presented in this report, so our past reservations, already conveyed to you in comments on your recent multiplexing and local service consolidation reports, stand. Briefly, our concerns were that the GAO analyses supporting this (consolidation) course of action omitted several factors crucial to the final cost determination.

However, now as then, we certainly would agree that better coordination among agencies and more centrally organized planning efforts are badly needed. Through better planning and coordination, we believe that economic benefits, even exceeding those identified by GAO in this report, can be achieved. With information technology related expenditures by agencies now probably approaching \$20 billion annually,

it would be entirely reasonable to expect that a comprehensive planning program, achieving even a minimal 10% efficiency improvement, could create annual savings in the billions of dollars.

In sum, we believe that this draft report brings some very important issues to the surface. However, we also believe that the presentation of these issues could be made more effective and the likelihood of follow-up action more concrete, were GAO to examine our above suggestions about providing more specificity and focus to your recommendations. If GAO chooses to pursue any of these suggestions, please feel free to contact Terry Steichen of my staff (724-3439) for any additional assistance.

Sincerely,



Stanley I. Cohn
Deputy Administrator for Operations

Enclosure



U.S. Department of Justice

JUL 17 1980

Mr. William J. Anderson
Director
General Government Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Anderson:

This letter is in response to your request to the Attorney General for the comments of the Department of Justice (Department) on your draft report entitled "A Federal Civil Agency Common-User Data Telecommunications Network--A Potential For Economies And Improved Data Protection."

The Department has reviewed the draft report, particularly pages 1, 45, and 48, which contain material pertaining to the Department, and concur with the information presented. However, because data telecommunications resources play a significant role in the Department's mission activities, we are also providing comments on two other important areas of the report.

1. With regard to the need for data telecommunications network security and protection, we agree in principle. As the report points out, many of the weaknesses in teleprocessing systems are related to human failings versus inadequacies of the systems themselves. Further, we agree that the National Telecommunications and Information Administration, or another "lead agency," should be charged with the responsibility for developing a national policy for data telecommunications security and protection criteria. However, it will be incumbent upon the "lead agency" to seek the advice and input of the civil agencies involved in order to satisfactorily accomplish its objective because of the various data types and levels of sensitivity involved from agency to agency.
2. The economies to be derived from shared systems are and have been, for some time, a source of extensive debate. As stated in the report, the General Services Administration (GSA), because of legislative restrictions, has not maintained the Advanced Record System (ARS) as a state-of-the-art system. At best, user agencies can only expect to meet their routine data telecommunications and administrative message requirements. Thus, for the transmission and reception of more urgent message traffic, individual mission-oriented agency systems are absolutely essential. Without such types of systems, many Federal agencies would be unable to meet their day-to-day operational requirements. Further, we doubt very seriously that GSA is in a position to accommodate, via ARS, mission-essential message traffic for the Federal Bureau of Investigation or Drug Enforcement Administration, or to expeditiously process aircraft movement messages for the Federal Aviation Administration. In order for the report to be more thorough and comprehensive, it should address mission-oriented systems. In

this regard, we note that the three systems cited on page 43 of the report are mission-oriented data telecommunications systems.

We appreciate the opportunity to comment on the report. Should you desire any additional information, please feel free to contact me.

Sincerely,



Kevin D. Rooney
Assistant Attorney General
for Administration

**UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE SECRETARY
OFFICE OF OPERATIONS AND FINANCE**

Washington, D.C. 20250

JUL 21 1980

Mr. Henry Eschwege
Director, Community and Economic
Development Division
United States General Accounting Office
441 G St. N.W.
Washington, D.C. 20548

Dear Mr. Eschwege:

The Department of Agriculture welcomes and appreciates the opportunity to review GAO's paper, "A Federal Civil Agency Common-User Data Telecommunications Network -- A Potential for Economics and Improved Data Security." Our review of the subject paper was made in light of our experience in conducting and coordinating major telecommunications studies and implementing and managing both dedicated and shared telecommunications networks. Further, our recent experience in the acquisition and user-cutover to a public data network (GTE Telenet) has given us good insight into the merits and problems of common-user data networks.

The Department offers the following general and specific comments and considerations on the subject paper.

1. We feel the paper places far too much emphasis on the Government's designing, constructing, implementing and operating its own data communications network. Our experience with Value-Added Services supports the observation that the Government needs to gain more experience in how to use network services and facilities, not how to implement and operate the same. The Department strongly recommends that the civil Government take advantage of the available commercial network service approaches to gain user experience before committing to any government owned and operated data communications network. This approach allows the Government greater latitude and does not commit the civil sector to possible static communications technologies. With the advent of integrated digitized voice and data communications networks, it seems especially inappropriate for the Government to embark on a long-range data communications design and implementation.

2. The subject paper advocates the need for a "comprehensive civil data communications study." In concept, the Department agrees with this conclusion and requests that agencies be included with GSA on the approach, type and magnitude of the study. However, we feel that the subject paper

Office of Operations and Finance is an Equal Opportunity Employer.

has drawn some conclusions which could only be drawn after the completion of such a study. For instance, the subject paper concludes (page 50, paragraph 2) that the present agency network environments are more expensive than a civil agency common-user shared service. The premise that continuing to aggregate users onto one common facility (i.e., agency-sharing to civil-government sharing) can reduce overall costs ignores the fact that tailoring a network facility to local needs can also reduce costs. Where the benefits of integration and aggregation versus local tailoring reside should be determined in the "comprehensive telecommunications study." If the subject paper's assertions are already substantiated, why, then, is the study necessary.

In general, it has not been verified that there will be overall cost reductions for an integrated civil shared network vice individual agency networks, shared or dedicated. The subject paper has drawn this conclusion based on the six agencies' experiences and studies. It should be noted that the Department's cost savings identified (page 45) were the result of a contractor study. Since this contractor has performed similar studies for three of the other agencies listed, the results may clearly reflect this contractor's views and biases, and not necessarily all factors.

3. We feel that the relationship which the subject paper attempts to establish between security requirements and the need or advantage of a civil integrated network has not been verified. We feel that the paper is advocating that the common user network is actually less vulnerable to compromise than agency-dedicated facilities. Again, only an exhaustive study could support or deny this assertion. In fact, the subject paper itself is ambiguous. In one instance, (page 33), the paper states that "use of common-user technology can provide greater protection than that in existing dedicated telecommunications networks procured separately by individual agencies". On the following page, however, the paper states that "the techniques used to assure data integrity and their primary implications are no different for a shared Government telecommunications network than for dedicated Government networks." The ability to "intercept and exploit data transmissions" is stated as being more difficult in a common-user environment; however, the same techniques used in common user networks (i.e., packet-switching and advanced routing techniques) are being applied to individual agency shared and dedicated networks.

4. Finally, we feel that the subject paper may be making an incorrect assessment concerning GSA's planning role in Government telecommunications. The paper states (page 3) that "there is no Federal agency which reviews and coordinates total civil Government telecommunications plans and requirements." However, it is the Department's understanding that GSA, under the auspices of various property management regulations, has the responsibilities of reviewing, and to some extent, coordinating, government telecommunications planning. In fact, the subject paper (page 45) notes that GSA has the responsibility for telecommunications planning, including studies and analyses. If there is presently no total review of civil Government telecommunications plans and requirements, perhaps it is due to the current mode of operation, and not because there is no agency given the responsibility for the same.

In summary, while we commend GAO for recognizing the need to examine civil Government data communications, we feel the subject paper requires revision before becoming the final report. Specifically, we request that the civil data communications study (1) place a minimum burden on the agencies, (2) not delay or impact on-going agency data communications efforts and (3) emphasize use of currently available shared networks versus emphasizing the designing, implementing and operating of government facilities. Again, we reiterate our concern that the Government may be set back several years technologically by designing and implementing a data communications network in the present fast-changing environment.

The Department is available for further discussion at your convenience. For additional information, please contact Victor Muller, telephone 447-4301.

Sincerely,



DEAN K. CROWTHER
Director



United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240

JUL 22 1980

Mr. Henry Eschwege
Director, Community and
Economic Development Division
U. S. General Accounting Office
Washington, D. C. 20548

Dear Mr. Eschwege:

Comments in the following paragraphs are offered after our review of the draft report entitled "A Federal Civil Agency Common-User Data Telecommunications Network -- A Potential for Economies and Improved Data Protection".

The suggestion that a shared civil Government data telecommunications network be developed offers a potential for significant dollar savings. In recognition of the potential savings to be realized through sharing of data communications facilities, Interior established a Departmental Data Communications Committee during October 1977. The primary task of this committee is to effect savings through the Department-wide sharing of data communications facilities, the exploitation of new technology or services, and combined acquisition of commonly used data communication equipment. The effectiveness of this action was recognized in GAO report #LCD-80-53 (5/14/80). Most of the Departmental facilities are operated at full capacity during the 6 a.m. to 6 p.m. period and therefore do not appear to be candidates for increased sharing. The use of statistical multiplexors and communications concentrators is encouraged to ensure the highest practical level of efficiency commensurate with operational requirements.

The Agency emphasizes the development of General Purpose ADP facilities which offer a wide range of data storage and processing capability to a varied community of users. The level of data security for each file is established during the implementation of the program. Accessibility is controlled within the host processor on which the data file resides. Many different data files may be accessed through the same physical terminal and associated data communications facilities. It is difficult to envision a variable accessibility level which would be controlled by the terminal or within the data communications facility, that could be adjusted to the level required for each file accessed. The alternative would be to set the level based on the requirement dictated by the most secure file to be accessed. This would place an unnecessary burden on the majority of users of that terminal.

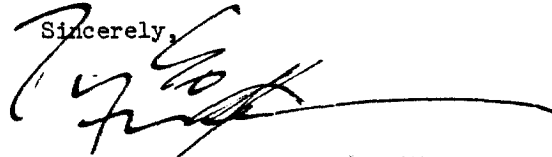
Mr. Eschwege
GAO

The use of state-of-the-art technological developments in services and equipment also provides the inherent advantage of increased security over long-haul facilities. This is made possible through the merging and compression of many separate data information streams into a single stream of apparently random information. If an intruder attempts to penetrate the system, the intrusion would have to be performed at either the terminal or computer end of the facility. This can be diminished through the use of normal physical and operational security procedures at the host computer and terminal sites.

The experience of AT&T in their work with the Advanced Communications System (ACS) and Xerox Corporation in the development of XTEN has shown that even large corporations who specialize in the area of data communications do not recognize the difficulties involved in an undertaking of this magnitude.

We appreciate the opportunity to provide comments relating to this report which will have a substantial impact on the future data communications and data security operating environments within the Civilian Agencies.

Sincerely,



Larry E. Meierotto

Assistant Secretary -
Policy, Budget and Administration



ASSISTANT SECRETARY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

JUL 28 1980

Dear Mr. Anderson:

The Secretary has asked me to respond to your request for comments on your Logistics and Communications Divisions draft report assignment, code 941159 on Civil Agency Data Telecommunications Networks.

We have reviewed the draft report and have no questions concerning the accuracy of the contents of the report, and we agree with its recommendations. Based on the findings of the report it appears that there may be economic advantages to having a shared civil government data communications network over continuing separate dedicated networks.

However, we feel there would also be disadvantages to a shared government-wide data telecommunications network and would appreciate an opportunity to provide an input to any study which may be performed as a result of your effort.

We appreciate the opportunity to review the draft report and look forward to participating in future studies.

Sincerely,

W. J. McDonald
W. J. McDonald
Assistant Secretary
(Administration)

Mr. William J. Anderson
Director, General Government Division
United States General Accounting Office
Washington, D. C. 20548

UNITED STATES INDEPENDENT TELEPHONE ASSOCIATION

1801 K Street, N.W. Suite 1201 Washington, D.C. 20006

(202) 872-1200

July 23, 1980

Mr. R. W. Gutmann
Director
U. S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Gutmann:

This is in response to your letter of June 20, 1980 which enclosed a draft report of Federal civil agency data telecommunications networks for our review and comment.

We concur, as a result of our review of the draft report, that a comprehensive study addressing the four topics identified on page iv would provide valuable planning information. Of particular interest are those topics concerning implications on the telecommunications industry and proposed management arrangements. We ask that our Association be afforded the opportunity to participate in such a study. The American Telephone and Telegraph Company and other major companies in telecommunications should also be invited to contribute.

We recommend that the methodology to be followed in developing the overall study include the concept of identifying similar functional mission requirements within the various government agencies that could reasonably be combined into a common user arrangement. We then suggest that such common user arrangements be the basis for considering a completely shared data telecommunication network for civil agencies.

We certainly appreciate the opportunity to comment on this important draft report.

Sincerely,



GEORGE E. PICKETT
Executive Vice President

ADAPSO

July 18, 1980

Mr. R. W. Gutmann, Director
Logistics and Communications
Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Gutmann:

This is in response to your letter of June 20, 1980 transmitting your draft report, A Federal Civil Agency Common-User Data Telecommunications Network -- A Potential For Economies And Improved Data Protection, for review and comment. This is a subject that is of great concern to ADAPSO members and we appreciate the opportunity to review the report and furnish our comments.

ADAPSO recommends that prior to beginning the study all pending legislative and regulatory action that will impact telecommunications in the Government be thoroughly considered. As you are aware, there are several actions presently taking place which will have a strong impact. The Congress is actively working on two bills H.R. 6121 and S. 2827 which may have a severe impact on telecommunication products and services for years to come. The FCC has issued its decision in the Second Computer Inquiry. H.R. 6410, the Paperwork Reduction Act of 1980, which establishes an Office of Federal Information Policy has passed the House and a comparable bill is expected to be voted out of the Senate this session. All three of these actions should be fully considered prior to undertaking a study of data telecommunication in the Civil Agencies.

Your report states "a shared data telecommunications network can, with proper controls, provide equivalent or better privacy protection than provided by existing civil Federal agency dedicated networks." We question how a single network could provide "better privacy protection" than multiple networks. You may want to reconsider this statement in the report.


Mr. Gutmann
Page 2
July 18, 1980

ADAPSO also urges that the scope of the recommended study include only data communication requirements among federal, state, and local government computer facilities. If there were any attempt to evaluate economies involved in the use of commercial teleprocessing services which include integrated telecommunications networks, it would require a separate study.

ADAPSO has a deep concern regarding the role of ATT in the recommended study and ATT's subsequent participation in any resulting Government data telecommunications network, ATT dominates all telecommunications services in the United States. It provides all or the overwhelming majority of the individual agency dedicated networks. The study team will have to have a close working relationship with ATT employees in order to complete its study. If a single civilian data communications network is recommended, how do you assure free and open competition in the procurement process? The pending legislation in Congress and the Second Computer Inquiry both generally address similar concerns.

It is obvious that a great deal of time and effort were required to produce this draft and we applaud your efforts and foresight into such a rapidly advancing technology. We appreciate the opportunity to work with you on this and all matters of mutual interest and concern. Please be assured of our desire to continue to work constructively with GAO.

Very truly yours,

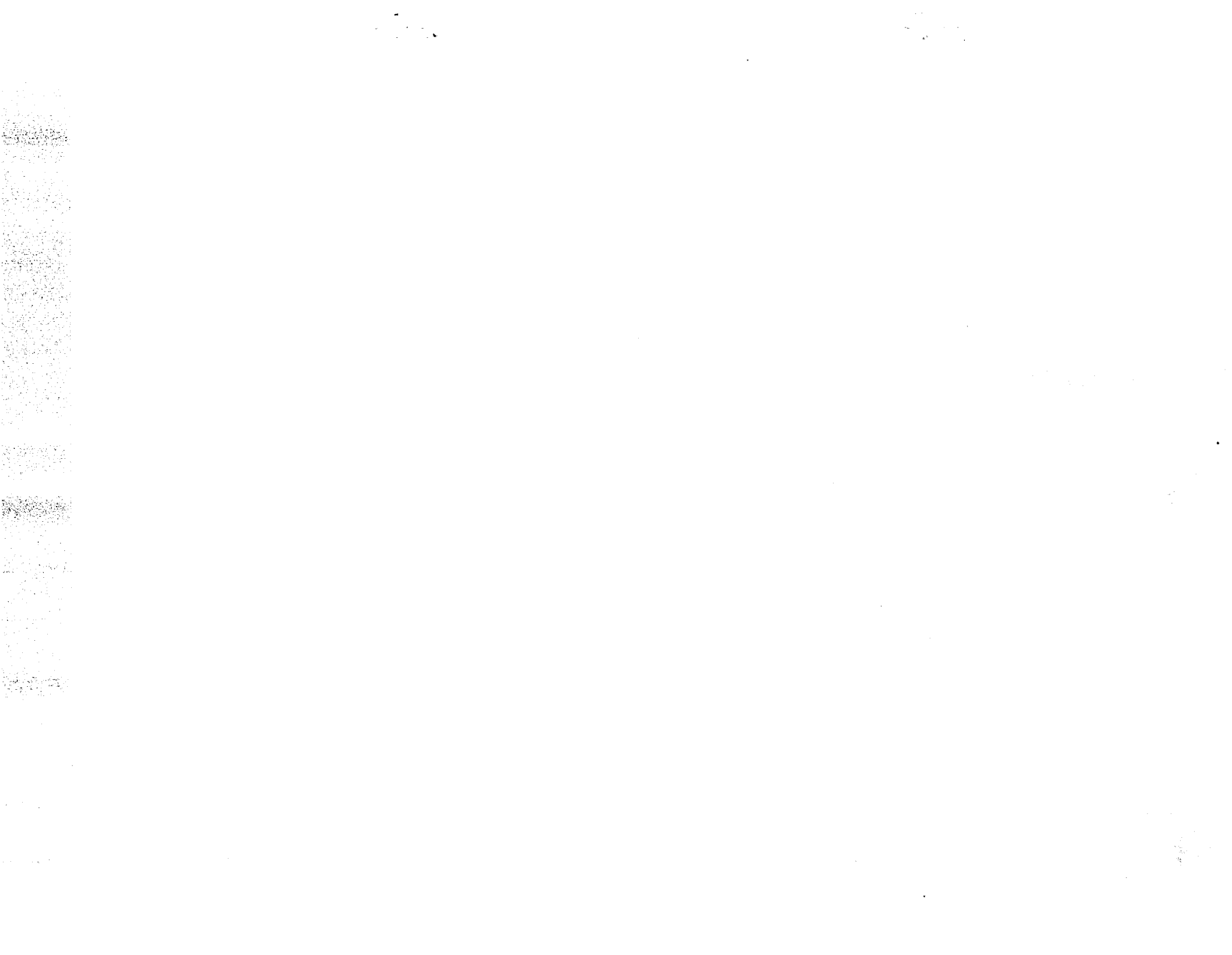

Warren E. Burton
Chairman, ADAPSO
Procurement Committee

bam



(941159)





AN EQUAL OPPORTUNITY EMPLOYER

**UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548**

**OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300**

**POSTAGE AND FEES PAID
U. S. GENERAL ACCOUNTING OFFICE**



THIRD CLASS