DOCUMENT RESUME

00050 - [A0591000]

Safeguarding Taxpayer Information: An Evaluation of the Proposed Computerized Tax Administration System. B-115369; LCD-76-115. January 17, 1977. 44 pp.

Report to the Congress; by Elmer B. Staats, Comptroller General.

Issue Area: Automatic Data Processing: Acquiring and Using Resources (102); Tax Administration (2700).
Contact: Logistics and Communications Div.
Budget Function: Miscellaneous: Automatic Data Processing (1001).
Organization Concerned: Department of the Treasury; Internal Revenue Service.
Congressional Relevance: Congress; House Committee on Ways and Means; Senate Committee on Appropriations: Treasury, Postal Service, General Government Subcommittee; Senate Committee on Finance.
Authority: Privacy Act of 1974 (5 U.S.C. 552a(e) (Supp. IV)). H. Rept. 90-1842. Internal Revenue Code of 1954, sec. 6103. Internal Revenue Code of 1954, sec. 7213.

The proposed IRS computer system, the Tax Administration System, was examined to determine safeguards for personal taxpayer information. Major threats to a network of this type are from untrustworthy users or from unauthorized access. Findings/Conclusions: Although absolute computer security is not practicable, the Tax Administration System will provide a high level of protection through technical, administrative, and physical controls. Some of the safeguards in the present system have weaknesses which should be corrected within the framework of existing security procedures. The use of crytographic devices will depend on an IRS determination based on its "risk and threat analysis," but present evidence does not indicate that the cost is warranted. Recommendations: Consideration should be given to: establishing a national data processing security office, guarding against unauthorized access, controlling employee access, improving physical security and control of information media, and seeking legal and other means to limiting disclosure of information. (HTW)

REPORT TO THE CONGRESS

BY THE COMPTROLLER GENERAL OF THE UNITED STATES

Safeguarding Taxpayer Information--An Evaluation Of The Proposed Computerized Tax Administration System

Department of the Treasury
Internal Revenue Service

The proposed Tax Administration System can provide a high level of protection for taxpayer information if the system is properly designed and implemented and if the weaknesses in the safeguards cited in this report are corrected.

LCD-76-115

JAN. 17, 1977

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-115369

To the President of the Senate and the
Speaker of the House of Representatives

This report assesses the concepts of the Internal Revenue Service's proposed computer system known as the Tax Administration System and its potential for providing protection for personal information. Further, the report evaluates the existing safeguards that have been identified for continuation under the proposed system. We made this review because of the extensive congressional concern for protection of individual privacy.

We made our review pursuant to the Budget and Accounting Act, 1921 (31 U.S.C. 53) and the Accounting and Auditing Act of 1950 (31 U.S.C. 67).

Copies of this report are being sent to the Director, Office of Management and Budget; the Secretary of the Treasury; the Commissioner of Internal Revenue; and the Administrator of General Services.

Comptroller General
of the United States

Contents

ABBREVIATIONS

ADP	automated data processing
GAO	General Accounting Office
IDRS	Integrated Data Retrieval System
IRS	Internal Revenue Service
RPA	resident programmer-analyst
TAS	Tax Administration System

GLOSSARY

Algorithm	A statement of the steps to be followed in the solution of a problem.
Application program	A computer program designed to accomplish a specific job or application such as payroll, inventory, etc.
Audit trail	A means of identifying and tracing actions taken in processing data. It encompasses the logging of selected events as they occur at specified points within a system.
Batch processing	A technique of data processing in which jobs are collected and grouped before processing.
Data base	(1) The entire collection of information available to a computer system and (2) a structured collection of information as an entity or collection of related files treated as an entity.
Data links	The interconnecting circuits operating on a particular method permitting exchange of information between installations.
Encryption	The transformation of data into secret coded symbols.
Flowchart	A graphic representation of the definition, analysis, or solution of a problem or situation.
Interactive	Pertaining to exchange of information and control between a user and a computer process, or between computer processes.
Machine language	A language a computer can use without translation.
Memory	The storage that is considered integral, internal, and primary to the computing system.
Object deck	A collection of punched cards representing a computer program in machine language.

Offline	Pertaining to operations that are independent of the main computer.
One-way encryption	The transformation of data into coded symbols without the ability to decipher or reverse the process.
Online	Pertaining to (1) equipment or devices under control of the central processing unit or (2) a user's ability to work with a computer.
Operating system	Software that controls computer operations including scheduling, debugging, input and and output control, accounting, storage assignments, data management and related services. Sometimes called the supervisor, executive, monitor, or master control program.
Parameter	A variable that is assigned a constant value for a specific purpose or process. For example, parameters may determine the number of characters in a field.
Realtime	Computation made while the related physical process is going on so that the results of the computation can be used in guiding the process.
Source deck	A collection of punched cards representing a computer program in a language designed for ease and convenience of expression. A generator, assembler, compiler, or translator must be used to transform the source language to machine language.
Switching point or center	A center where messages are relayed or routed according to data contained in the message or according to specific operating instructions or programs.
Transaction-oriented system	As used herein, a transaction-oriented system is one that permits a user only to input and receive data. The input and receipt of data is controlled by application programs. The users' interaction with application programs is achieved by means of macroinstructions which isolate the user from direct access to such programs.

COMPTROLLER GENERAL'S
REPORT TO THE CONGRESS

SAFEGUARDING TAXPAYER INFORMATION--AN EVALUATION OF THE PROPOSED COMPUTERIZED TAX ADMINISTRATION SYSTEM

D I G E S T

This report assesses the capability of the proposed Tax Administration System of the Internal Revenue Service to provide appropriate technical, administrative, and physical safeguards on taxpayer information as required by the Privacy Act of 1974 and other legislation. Congress may wish to consider restricting linking or interfacing of the system with other systems and prohibiting terminals outside of the Internal Revenue Service. (See p. 38.)

A separate report has been issued on GAO's evaluation of the reasonableness of the cost-benefit analysis for the proposed system.

The Internal Revenue Service collects virtually all Federal taxes. It has over 80 thousand employees and processes approximately 125 million returns annually. The Service converted to the current automated data processing system during the 1960s because the workload was increasing at such a rate that conventional manual and machine processing could not do the job. The system has been changed and adapted over the years to meet frequent legislative changes, workload growth, and increasing program demands. (See p. 1.)

According to Internal Revenue officials, the automated data processing system was based on early technology; later improvements have been largely piecemeal. This development resulted in considerable duplication of effort and inefficient operations. Consequently, in November 1973, the Commissioner of Internal Revenue advised the Department of the Treasury that the existing system needed to be completely redesigned. The Office of Management and Budget granted

program approval in September 1975 to acquire a new computer system, to be known as the Tax Administration System. (See p. 2.)

GAO evaluated the Tax Administration System concept and its potential for protecting taxpayer information. Existing technical, administrative, and physical safeguards were analyzed under the assumption that they can and should be continued. (See p. 4.)

Absolute computer security is not now technically possible, but even if it were, the highest level of protection attainable is rarely practicable, considering the cost involved. (See p. 6.)

Through proper design and implementation, the Tax Administration System will be able to provide a high level of protection for taxpayer information. (See p. 9.) However, selected technical, administrative, and physical safeguards now used have a number of weaknesses which should be corrected within the framework of existing security procedures, methods, and controls.

Evidence does not show a present threat to taxpayer information that would warrant the cost of procuring special cryptographic devices. IRS has begun a "risk and threat analysis" which must be completed before any decision is made as to use of cryptographic technology. (See p. 31.)

To provide the security needed for the proposed system, GAO recommends that the Commissioner of Internal Revenue:

--Establish a national data processing security office and a similar office at each data processing facility responsible for administrative, physical, and technical security. (See p. 35.)

--Consider ways and means to protect taxpayer data from improper access by

non-IRS employees with access to a facility where taxpayer information is maintained. (See p. 22.)

--Require mandatory periodic updating of background investigations of employees using or having access to taxpayer information, to make sure that their activities warrant the Government's continued trust. (See p. 22.)

--Initiate procedures to provide appropriate accountability and control of all magnetic tapes, microfilm, and other information media. (See p. 22.)

--Require periodic evaluations by the national office (IRS headquarters) of the effectiveness of physical security at each service center and the National Computer Center. (See p. 27.)

--Eliminate, where possible, lists of employee identification data used to gain access to the computer system and use one-way cryptographic messages to safeguard the data files containing that identification information. (See p. 16.)

--Provide additional restrictions on computer terminal users, to permit them access only to those functions and data necessary to their duties. (See p. 16.)

--Initiate controls over the activities of employees with the technical training necessary to circumvent security safeguards. (See p. 16.)

--Seek legal authority to withhold from public disclosure data processing documentation that would aid illegal access to taxpayer information. (See p. 16.)

--Establish appropriate controls to make sure that only authorized interservice center activity is permitted. (See p. 32.)

--Require supervisory approval for all out-of-district inquires (1) to taxpayer accounts by taxpayer compliance employees and (2) to inactive accounts by taxpayer service representatives. (See p. 16.)

--Study the feasibility of further system constraints such as additional requirements a terminal user must meet before gaining access to a taxpayer's account. (See p. 16.)

--Insure that communication risks and threats are completely analyzed before deciding whether to purchase sophisticated security devices. (See p. 32.)

AGENCY COMMENTS AND ACTIONS

The Commissioner of Internal Revenue generally agrees with GAO's recommendations and has taken various actions to correct the reported weaknesses in safeguards for taxpayer information. (See pp. 16, 22, 27, 32, 35, and app. I.)

CHAPTER 1

INTRODUCTION

MISSION AND ORGANIZATION OF THE INTERNAL REVENUE SERVICE

The Internal Revenue Service (IRS) is under the Department of Treasury with a mission of administering and enforcing the internal revenue laws. The Service has the responsibility of collecting virtually all Federal tax revenues.

The IRS organizational structure is decentralized with the national office in Washington, D.C.; the Data Center in Detroit, Michigan; the National Computer Center in Martinsburg, West Virginia; and seven regional offices located in major cities across the country. The regional offices supervise and coordinate the activities of 58 district offices and 10 service centers. In addition, there are approximately 900 local offices functioning as satellites of the district offices.

To accomplish its mission, IRS has more than 80,000 employees and processes approximately 125 million returns annually.

OVERVIEW OF CURRENT INFORMATION HANDLING ACTIVITIES

IRS converted to automated data processing (ADP) because statistics showed that the Service's workload was increasing beyond the capacity of conventional manual and machine processing capabilities. The Commissioner, in February 1959, presented an ADP program to the Congress and received House and Senate budget approval in June 1959. The system was implemented during the 1960s and has been changed and adapted over the years according to frequent legislative changes, workload growth, and increasing program demands.

Although the IRS organizational structure is decentralized, the data processing structure within the Service is centralized with all taxpayer master files maintained at the National Computer Center.

Under the current system, taxpayers file returns directly with the service center in their geographic area. The centers put tax data on magnetic tapes and perform certain editing and verification checks. The tapes are sent to the National Computer Center for further processing. In addition, substantial offline activity occurs at the centers which

includes the preparation and processing of taxpayer correspondence and accounting for tax returns and moneys received.

According to IRS officials, the original ADP system was based on early technology, and subsequent enhancements have consisted largely of piecemeal improvements. This development has resulted in considerable duplication of effort and inefficient operations. The heart of the problem, according to IRS, lies in the master files of the present system which prohibit ready access to tax account data required to answer taxpayer inquiries and meet other IRS program needs.

Consequently, in November 1973, the Commissioner of Internal Revenue advised the Department of the Treasury that the ADP structure of their existing system needed complete redesigning. Program approval to acquire a new computer system was granted by the Office of Management and Budget in September 1975.

THE PROPOSED TAX ADMINISTRATION SYSTEM (TAS)

The proposed new system calls for extensive use of interactive online processing and the decentralization of the tax account master files from the National Computer Center to the 10 existing service centers. The National Computer Center is to be redesignated the National Communications Center. It will maintain a centralized account directory and backup master files, and serve as a switching point for transmission of data between service centers. User terminals are to be located in the service centers and various field offices.

The Service's principal objective of the redesigned system is to provide more responsive service to taxpayers and IRS functional activities by accelerating return processing and by providing increased information for taxpayer inquiries and operational needs of the Service. An essential element of the new service-oriented system is quicker access than in the past to more current information by employees of more IRS offices.

LEGAL REQUIREMENTS

The Internal Revenue Code of 1954 imposes certain responsibilities upon taxpayers and others to furnish tax returns and related information to the IRS. The code requires the Service to determine the correctness of returns and other

information received, to secure or prepare delinquent returns, and to collect unpaid taxes. It also imposes criminal sanctions such as imprisonment and/or a fine plus dismissal of Federal employees guilty of unauthorized disclosure of taxpayer information.

The Privacy Act of 1974 requires the Service to establish appropriate technical, administrative, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

CHAPTER 2

THE TAX ADMINISTRATION SYSTEM CONCEPT AND DATA SECURITY

The capability of an information processing system to protect personal data is contingent upon the use of adequate technical, administrative, and physical safeguards. The protection of data must be considered from a total system perspective; that is, the protection of data must be considered from its origination to its final destruction. Since the proposed Tax Administration System has not been implemented, a complete evaluation cannot be made as to its ability to protect the privacy of individual taxpayer information.

What is possible is to evaluate the concepts of TAS and their potential for providing high-level protection of personal information. Further, the existing technical, administrative, and physical safeguards can be analyzed to identify pertinent safeguards to be continued under TAS. This chapter discusses the TAS operating concept and its ability, if properly designed and implemented, to protect personal information. However, the conclusions drawn from this review should not be construed to apply to other computer systems operated by IRS, such as those supporting the Service's administrative and intelligence functions.

THE TAS OPERATING CONCEPT

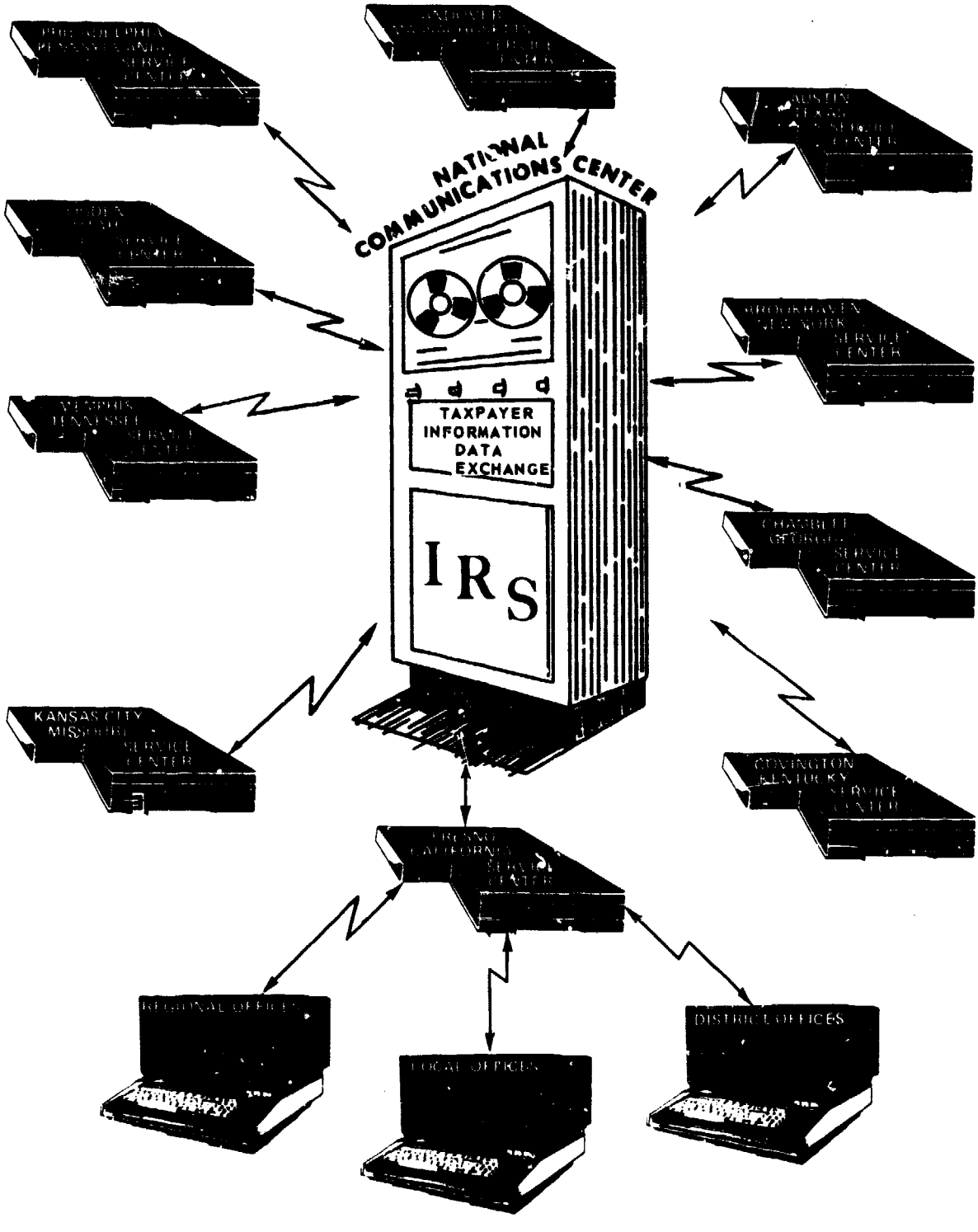
The TAS concept envisions a batch and realtime transaction-oriented computer network employing a decentralized data base. The network will consist of over 8,000 terminals, 10 service centers, and 1 communication center as shown in figure 1.

Each service center will maintain selected information pertaining to taxpayers with a primary address within the center's geographic area of responsibility. High volume input to the data base will be through the Direct Data Entry System currently in use with approximately 5,000 terminals but without access to taxpayer accounts. Information from tax returns and tax payments will be entered through the Direct Data Entry System terminals and the output will be used to post and update the master file maintained in the data base.

Terminals located in the service centers and IRS regional, district, and local offices will have direct access to taxpayer information in the data base maintained for their

FIGURE 1

OVERVIEW OF THE PROPOSED TAX ADMINISTRATION SYSTEM NETWORK



geographic area. Controlled access to taxpayer data maintained at other service centers will be possible through use of the communication network and the facilities of the proposed National Communications Center. The processing will primarily involve inquiries and transactions, such as adjustments to taxpayer accounts.

Mathematical verification, validity checks, balancing, and other data controls occur prior to or during posting operations. The accounting function will be accomplished as the transactions are processed and files updated. Over 45 types of tax returns and more than 300 different transaction categories are included in this extremely complex operation.

COMPUTER SECURITY IN THE TAS ENVIRONMENT

The state-of-the-art in computer security is such that absolute security has not been achieved. However, absolute security would rarely be practicable in any environment regardless of whether humans or computers are used considering the costs that could be involved in attempting to achieve the highest level of protection.

Decisions on security must essentially identify and define the level of protection which makes the cost greater than the benefits--either in monetary or punitive terms--of subverting a system. We believe reasonable protection can be provided for taxpayer information by increasing the cost to an unacceptable level of subverting the system and by imposing heavy penalties for those who make unauthorized or inappropriate disclosures of taxpayer information. The various system safeguards discussed in this report will make it more difficult to successfully subvert a system. Further, there are a number of laws, not discussed in this report, that have been enacted by various jurisdictions which provide criminal sanctions for such acts.

In analyzing the potential for TAS to provide an acceptable level of protection for taxpayer information, it is important to review the type and nature of the major threats to a transaction-oriented, dedicated computer network. In addition, the ability of a transaction system to cope with these threats must also be evaluated, particularly where the system employs a decentralized data base.

ANALYZING THE THREATS

The major threats to a dedicated computer network such as TAS stem from two sources--(1) authorized, but untrustworthy users and (2) malicious penetrators. Their motives are the same, but the untrustworthy user is an individual who has authorized access to the data of interest while the malicious penetrator, whether an employee or not, is not authorized access.

The problem of the untrustworthy or dishonest employee is not unique to automated data processing systems. Only the concentration of data in such systems increases the risk over noncomputerized systems. Protection against the untrustworthy user can be accomplished through well-designed security safeguards which include personnel screening, activity monitoring, and effective auditing. These and other controls are discussed below and in subsequent chapters of this report.

The malicious penetrator presents a different threat than the untrustworthy employee in that technical security measures must be circumvented. In order to place the threat from this source in perspective, it is necessary to understand how a penetrator would achieve his objective and what skills he must possess.

According to the technical community, a penetrator circumvents computer security by calling on an operating system function in a way unanticipated by the designers. He is frequently aided by the fact that designers of operating systems normally assume that users will not deliberately attempt to force a malfunction of the system.

The penetrator may achieve his objectives by either (1) acquiring a list of terminal user identifiers and corresponding passwords or other identification and confirmatory information maintained within a computer file or (2) obtaining supervisory (executive or master) control of the computer system. Using the first method, the penetrator is able to masquerade as any of the authorized users, while use of the second method gives him direct access and control of any file or program in the system.

In order for a penetrator to accomplish his objective by either method it is necessary that he be moderately skilled in programming, expend time and effort to understand rather complex operating systems, and have knowledge of the limitations that occur in the design and implementation of the systems. Such knowledge suggests to a penetrator where to

look for possible errors and design flaws. If he has access to system documentation, his ability is considerably enhanced.

Against such individuals, contemporary computer operating systems generally fail to provide adequate protection for personal or sensitive information because of the penetrator's ability to exploit design flaws. How then can TAS provide protection against such a threat?

SECURITY IN A REALTIME TRANSACTION SYSTEM

Generally, the risk of a successful penetration increases with the flexibility provided the users of the system. The system user constraints needed in TAS are summarized below and are discussed in more detail in Chapters 3, 4, and 5. It is these constraints the penetrator must circumvent to gain access to taxpayer information.

In order to significantly reduce the risk, the TAS concept sharply curtails the users' ability to manipulate the system by removing their capability to enter a program over a terminal. Such systems, if properly designed and implemented, can effectively isolate the system from the threat posed by individuals with programming knowledge (i.e., the penetrator).

Under the TAS concept, a terminal operator, after obtaining access to the system, may enter, change, and retrieve data according to a limited number of command codes. Each command code performs a specific function in relation to the information entered and the data maintained on the system. For example, one command code used in conjunction with appropriate input data may cause a taxpayer's account data to be displayed while another may effect an adjustment to a specific data element.

The flexibility of the transaction system is further reduced in TAS through use of employee and terminal profiles. Such profiles can restrict terminal users to only those command codes and terminals necessary for them to perform their specific duties.

By limiting the terminal user to transaction processing, application programs and their modifications must be placed on the system under tightly controlled conditions, preferably at the computer center. Here it is necessary to isolate the programmer from the system by requiring all programs and program changes to be submitted to an independent test and evaluation group. This group provides an interface between the

application and systems programmers and the computer operations. They review, validate, and approve all programs to be placed on the system and therefore act as a control over the activities of the programming function.

As with any system, a transaction system such as TAS must be well designed with security as an objective. Access controls must be adequate, parameter checks should be extensive, and audit trails must be employed. Physical identification is also desirable, and under TAS, an identification badge which can be read and validated by the computer will be used as one step in activating a terminal and identifying the user.

This approach provides a high level of protection to taxpayer information by isolating the system from the programmer and reducing the risk by restricting the terminal user to only those functions necessary to process authorized transactions. Security of a transaction system such as TAS is not dependent on vendor-supplied features and mechanisms but rather on good system design, operating procedures, and program testing.

CONCLUSIONS

While absolute security is generally not achieveable in contemporary operating systems, we have concluded that the TAS concept is capable of providing a high level of protection against the technical threat posed by the malicious penetrator. However, providing only technical protection will not adequately safeguard taxpayer information and thus will not comply with the Privacy Act of 1974. Consideration must also be given to the administrative and physical safeguards as well as the technical controls. The following chapters in this report discuss our review of selected technical, administrative, and physical safeguards provided by the current IRS information system since these constitute the environment in which TAS, also, will operate. The improvements considered necessary under TAS will also be discussed in those chapters.

CHAPTER 3

TECHNICAL CONTROLS

The major elements of security in a transaction system such as the proposed Tax Administration System lie with the ability of the system to control access, limit user privilege, and maintain program integrity. The capability of TAS to adequately perform these functions cannot be conclusively evaluated prior to system design and implementation. However, IRS Integrated Data Retrieval System (IDRS) is a transaction system currently in use that has security requirements similar to TAS.

IDRS is a data terminal system used at each of the 10 service centers and certain field offices. This system is intended to be replaced by TAS. IDRS, through the use of computer terminals, provides immediate access to selected information in about 10 percent of the taxpayer master records. The selection of records to be placed on this system is based on the probability of taxpayer inquiry and IRS need. IDRS also provides a user the capability to gain access to any of the remaining taxpayer master records by having the information extracted from the master files at the National Computer Center.

An evaluation of the technical security design and implementation of IDRS disclosed the need for security improvements that should be considered during the development of TAS.

DATA TERMINAL ACCESS CONTROLS

Access to IDRS through a data terminal is controlled through use of terminal and employee profiles. Such profiles are tables maintained on the computer system that contain the specific attributes for each terminal and each authorized user. The terminal profiles restrict the use of a terminal to certain functions. The employee profiles contain the information necessary to identify authorized users of the system and to restrict those users to executing only authorized commands. One of the major elements of the identification process is the unique employee password which is used in activating a terminal.

A special computer program generates the passwords for all authorized terminal users and produces a list of alternate passwords to be used in the event a password is lost or compromised. Passwords are periodically changed and new passwords are furnished to the employees in sealed envelopes by the security administrators at each service center.

A master password list is maintained by the security administrator and each employee's password is contained on the computer system in the employee profile security file. A backup copy of this file is maintained on magnetic tape for recovery purposes in the event of an emergency.

Access to an employee's name and password through either the assignment and distribution process, master password list, or the employee profile security file would permit a penetrator or dishonest employee to gain access to the computer system by masquerading as that employee. It is the initial step in gaining access to information in the system. Currently the security administrators and their staffs, the resident programmer-analysts (RPAs), and the computer operators either have access to listings of this information or can readily obtain such listings.

Protection of password and other identification data can be enhanced by IRS eliminating the ability to produce listings of assigned employee passwords. This enhancement can be accomplished by fully automating the password generation, assignment, and distribution process, thus providing for computer-generated passwords with the record maintained in the computer. Further, the employee profile security file can be protected by employing a one-way encryption scheme whereby identification data is maintained and used by the computer system in a form that would be unintelligible to an individual even if purposely or inadvertently printed.

CONTROLS OVER ACCESS TO TAX INFORMATION

Under the current system, an IDRS terminal user has access to information on virtually any taxpayer in the country. At any one time, IDRS provides online access to selected information in about 10 percent of the master file. However, a request for tax information on almost any taxpayer can be made through the system and the information will be extracted from the centralized data base at the National Computer Center and forwarded to the requesting service center.

TAS will decentralize the data base and each service center will maintain selected information pertaining to taxpayers with a primary address within the center's geographic area of responsibility. This will automatically restrict data access without supervisory or second party intervention to addresses in that service center area--about 10 percent of the total information currently available through IDRS. The transfer of

information between data bases maintained at the service centers will require supervisory approval under TAS. This approval process can be automated and provide even more effective control over interservice center activity. (See p. 32.)

In our opinion, IRS district and local office terminal users' access to information can be further constrained under TAS without seriously impeding operations. The two functional areas affected by additional constraints would be taxpayer service and taxpayer compliance. Each of these functional areas has different information requirements and therefore must be considered separately. The following is an example of how each can be further limited as to the taxpayer information they may have access to without supervisory approval.

Taxpayer compliance includes such areas as audit and collections. The preponderance of taxpayer information needed by IRS employees to perform this function is confined to the geographic district in which they are assigned. Therefore, TAS can restrict employees working in the compliance area to only those taxpayer accounts with a primary address within the IRS district involved. Out-of-district inquiries should require supervisory approval. Since there are 58 districts, this would limit a district or local office employee to an average of less than 2 percent of the total taxpayer accounts.

Taxpayer service presents a different problem as the contact is normally initiated by the taxpayer. Typical inquiries would include status of refunds or amounts due the Government. Here, the taxpayer service representative can be restricted to two categories of taxpayer accounts--(1) those active accounts maintained by the host service center where money is either due to or due from the taxpayer and taxpayer contact can reasonably be expected and (2) those inactive or zero balance accounts with a primary address within the servicing IRS district. Out-of-district inquiries on inactive accounts should require supervisory approval. There are 58 districts, and only about 10 percent of the files have been maintained in an "active account" status. Therefore, the taxpayer service representative at a district or local office, within each of the 10 service center areas, would be limited to an average of less than 3 percent of the total taxpayer accounts.

In those instances where supervisory approval would be required, automation of the validation process would, in our opinion, provide the most effective control. A supervisor would be required to enter into a terminal the validation data that would release each individual request, thus precluding an employee from obtaining taxpayer information without independent confirmation as to need.

CONTROLS OVER ASSIGNMENT AND USE OF COMMAND CODES

Command codes activate computer routines for processing of data and inquiries. Each code performs a specific function in relation to the transaction entered and the data maintained in the system. The number and combinations of command codes an employee is permitted to execute determines the capability of the user to process or obtain data from the system.

One of the major elements of security in a transaction system is the limitation of the privileges given a user. This has been recognized by IRS and its regulations stipulate that IDRS users possess only those command codes required by them to perform their specific duties. Our review at the Brookhaven and Covington Service Centers disclosed numerous instances where employee profiles contained codes in excess of those required. For example, our review of the distribution of five command codes at the Brookhaven service center disclosed 67 employees having command codes in excess of the authorized. An interview of 21 employees at the Covington Service Center revealed that over half did not use or need one or more of the command codes in their profiles.

The administrative procedures were not being followed for authorizing changes to command codes contained in employee profiles. IRS regulations require that all changes be documented and approved by the IDRS security administrator. Out of 361 changes to employee profiles at the Covington Service Center, 344 cases were not properly documented. A similar situation was found at the Brookhaven Service Center where documentation was not on file with the security administrator for over 50 percent of the changes examined. Failure to properly implement IRS regulations in this area can result not only in employees having excessive system privileges but places the security administrator at a disadvantage in attempting to identify those users with excessive system privileges and in initiating appropriate action to limit their access only to those parts of the system needed to perform their assigned duties.

We were informed that, in part, possession of excessive command codes by employees resulted from the operational necessity to transfer employees from one branch to another because of workload. This was particularly true where an employee was temporarily loaned to another branch. In such situations, additional codes were often authorized without full regard for the codes the employee already possessed. This resulted in employees not only having excessive command

codes in their profiles but also combinations of codes that permitted extensive access and processing capability.

Partially automating the process can significantly enhance the security in this area under TAS as well as under IDRS. Since the IRS employee number contains a designation of the branch in which an individual works, the system can be programmed to (1) automatically delete the command codes contained in an employee profile upon change in employee number and (2) add to the profile those command codes which are common to all employees of the new branch. Additional command codes would require manual approval and processing. Further, compatibility tests should be included that would prevent an individual employee from holding certain combinations of command codes that would provide excessive system privileges.

COMPUTER PROGRAM INTEGRITY

System and application programmers can do more damage to a system with less chance of being caught than almost any other person involved with data processing. It is therefore necessary to isolate the system from the programmer in order to provide any degree of security. IRS computer programs are developed by the national office and distributed to the service centers and the National Computer Center. RPAs are assigned to each location to maintain the production programs for IDRS as well as other computer operations. The maintenance is in the form of corrections of program errors, changes to program variables and constraints, and modifications to processing logic. All changes and modifications to programs require approval of the national office.

We found the controls exercised over the activities of the RPAs to be practically nonexistent. For example, the following conditions were observed at one or more of the data processing facilities visited.

--RPAs had access to the computer, tape library, object decks, flow charts, program listing, and source decks.

--No controls were exercised over the data an RPA could list or the use made of the listing.

--RPAs are not restricted in their ability to obtain listings of information contained in the computer memory.

--Independent reviews and evaluations of program changes were not conducted.

--A program change was made without the required approval from the national office.

--Periodic comparisons of master programs at the national office were not made with those at the computer facilities.

While considerable effort has been devoted to controlling access to the computer system through data terminals, little attention has been given to controlling the activities of the RPAs. Under current procedures, the RPAs have both the technical ability and the opportunity to manipulate the data system without readily being detected.

Proper control procedures should require that the RPAs be isolated from the data system by (1) requiring all computer programs and program changes to be approved, submitted for an independent test and evaluation, and placed on the system only under tightly controlled procedures, (2) preventing all RPAs from handling computer-room hardware, and (3) monitoring all programmer activity to include periodic verification of the programs residing on the system files.

DATA PROCESSING DOCUMENTATION

IRS has publicly disclosed a large volume of data processing documentation in accordance with the Freedom of Information Act. Included in this category are manuals on the description and operation of the data system and the data elements and codes used.

Such disclosure of the data processing documentation permits a potential penetrator to study the system for possible flaws that could be exploited to gain unauthorized access to taxpayer data. Further, possession of this documentation permits anyone to interpret any taxpayer information they are able to obtain.

The need to protect system documentation that would aid a potential penetrator can be illustrated by the nationally publicized case involving the theft of equipment from the Pacific Telephone & Telegraph Company. In this case, access to the company's computer was gained from studying an outdated manual found in a trash container that detailed how the computer inventory system worked.

CONCLUSION

The use of terminal and employee profiles limits the general access to the data system and permits the terminal

users to address only that data necessary to perform their duties. The effectiveness of these controls has been diminished by weaknesses in implementation of IRS regulations relating to limitations to be placed on user capability. Further, the lack of control over the activities of technically trained employees and the public release of data processing documentation are major weaknesses in the overall security of the current data processing system. The security deficiencies and weaknesses found in the present system and discussed in this and the two succeeding chapters are shortcomings that, in our opinion, can be corrected within the framework of existing security procedures, methods, and controls.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

We recommend that all human interaction with the data system be evaluated by IRS and appropriate controls established in the existing system and under TAS to preclude any individual from obtaining unlimited or excessive system capability. Specifically, eliminate, where possible, lists of employee identification data used to gain access to the computer system and use one-way cryptographic messages to safeguard the data files containing that identification information. Further, the assignment and deletion of command codes from employee profiles should be automated to the maximum extent practical under both the present system and TAS. Appropriate controls should be programmed to prevent an authorized user from holding certain combinations of command codes which would, in that combination, violate the principle of segregation of duties.

Constraints should be imposed under TAS on the individual terminal operator's ability to gain access to taxpayer information. As a minimum, we recommend that TAS be designed to require supervisory approval for (1) all out-of-district inquiries on inactive accounts by taypayer service representatives and (2) all out-of-district inquiries by taxpayer compliance employees. The use of further constraints such as additional information a terminal user must know in order to gain access to an account should be studied by IRS. The objective of such a study should be to identify practical methods that can be used to control access to individual taxpayer accounts.

We further recommend that positive controls be exercised over the activities of those employees that have the technical training necessary to circumvent the security safeguards. In addition, IRS should seek legal authority to withhold from

public disclosure those elements of system documentation that would substantially enhance the ability of unauthorized individuals to gain illegal access to taxpayer information.

AGENCY COMMENTS AND ACTIONS

The Commissioner of Internal Revenue stated that, as a result of their own internal audit findings and the GAO recommendations, they had eliminated the lists of employee access identification data and were encrypting such data in the computer files as a further safeguard. In addition, they have taken steps to automate the assignment and deletion of command codes assigned to terminal operators. Techniques of fully automating the password generation, assignment and distribution process, and the more secure one-way encryption of all access data and files were being explored for possible use in the future.

The Commissioner agreed with the principle that terminal users should not have access to more tax account data than is necessary to perform their assigned duties. He stated that IRS had initiated a study to thoroughly explore all aspects of the subject. The objective of the study is to identify practical ways to limit access to data without adversely affecting service to the public or productivity of the terminal users or their supervisors. Further, IRS is to continue to evaluate the use of additional positive identifiers of terminal users (beyond badge, password, and employee profile controls). Also being considered is a requirement for supervisory terminal validations and counter authorization for access based on geographic areas or levels of account activity.

IRS recognized the vulnerability of the ADP system to those employees that have the technical training necessary to circumvent security safeguards. They are considering various methods and procedures to control the activities of such employees and balance security concerns with the need for employee efficiency. In addition, IRS has initiated a review of ADP documentation to identify materials which, for security reasons, should not be publicly disclosed. The Commissioner stated that if the Service finds that current exemptions of the Freedom of Information Act do not offer sufficient protection to sensitive ADP material, appropriate legislation will be sought.

CHAPTER 4

ADMINISTRATIVE CONTROLS

The general objective of an agency's system of controls is to make sure that the duties and responsibilities imposed by law are executed as effectively, efficiently, and economically as possible. To meet this objective, certain principles and requirements must be observed in establishing qualifications and obtaining suitable employees. All other elements of administrative controls are designed to control the activities of officials and employees of the agency.

Personnel controls should reflect the need for careful selection of mature and trustworthy employees. Within IRS, new employees are subjected to pre-employment screening. This is accomplished through a routine investigation required for all prospective Federal employees. Where sensitive positions are involved, IRS's investigative organization is required to conduct appropriate background checks. The extensiveness of the screening is dependent, in part, on the sensitivity of the positions being filled.

Once employed, the activities of IRS employees are controlled through internal checks and balances. The current system provides:

--Extensive data and accounting controls to make sure that (1) tax returns and related documents are properly processed, (2) tax data accuracy is maintained throughout the various processes, and (3) errors are promptly detected and corrected.

--Audit trails disclosing who had access to the system and what taxpayer records were involved.

--Internal reviews of operations.

A review of selected administrative controls employed at the IRS service centers and the National Computer Center disclosed the following areas where improvements are considered necessary.

BACKGROUND INVESTIGATIONS

IRS regulations state that the security investigation program is designed to provide information about an individual's background commensurate with the degree of responsibility and trust imposed by the position to be held. The scope

of investigation varies from local police checks to complete background investigations. The investigations are performed either through the Office of the Assistant Commissioner (Inspection) or by the Civil Service Commission.

New employees, with the exception of those applying for temporary employment of 90 days or less, receive a National Agency Check and Inquiry investigation conducted by the Civil Service Commission. This includes a check of the Federal Bureau of Investigation, Civil Service Commission, military, and other Government agency records. IRS also verifies that new employees have paid their Federal taxes for the 3 years prior to their application.

Applicants for specified positions and those on whom derogatory information was uncovered receive, in addition to the above, an extensive character investigation. The investigation covers the 10 years preceding the date of the request for investigation or from the individual's 18th birthday, whichever is shorter. It includes interviews with neighbors, former employers, supervisors, co-workers, references, and educators; a check of police and credit agencies; and foreign travel verification through the State Department. IRS also audits their income tax returns for any 2 years prior to the date of application for which the statute of limitations has not been invoked.

Specified positions are defined as (1) grades GS-9 and above--employees earning $6.78 or more per hour, (2) all computer personnel, and (3) all personnel in inspection and intelligence. Seasonal employees holding these positions receive the same type of investigation.

Applicants for temporary positions of 90 days or less receive only a police and an FBI name check. This involves a search by local police and FBI for arrest records of incidents that should be known to IRS.

While the above procedures appear to be adequate, periodic reinvestigations are not conducted on any service center or National Computer Center employee after the initial investigation. We believe such updates should be made to insure that the activities of the individual employees have been such as to warrant the Government's continued trust. Such periodic updating is required by many agencies for employees handling national security information.

The major discrepancy in the personnel screening process does not lie with the background investigations afforded IRS employees but rather with the absence of security investigation for non-IRS employees such as the computer equipment

maintenance personnel. Many of these individuals are permitted unescorted access to the service centers and the National Computer Center and have the same, or possibly greater, opportunity as the IRS employees working in the facilities to extract sensitive taxpayer information.

We were informed that IRS had addressed, on several occasions, the lack of security clearance for non-IRS employees. They presently take no position as to whether or not they have the authority to require background investigations for non-federal employees. We believe that the Privacy Act of 1974 and the statutes limiting disclosure of taxpayer information and returns provide sufficient authorization for IRS to include provisions in their contracts requiring appropriate background investigations of contractor employees having access to facilities where taxpayer information is maintained. The authority for such investigations is found in sections 6103 and 7213 of the Internal Revenue Code of 1954, as well as provisions of the Privacy Act of 1974, 5 U.S.C. 552a(e) (supp. IV, 1974).

CONTROLS OVER INFORMATION STORAGE

IRS information is stored in various ways--documents, magnetic tapes, magnetic disks, and microfilm. TAS will use these same types of storage. Controls exercised over such storage need improvement at several of the locations visited.

The master [illegible]nd associated records are maintained on over 100,00[illegible] magnetic tape at the National Computer Center. To reduce the possibility of loss or compromise, it is necessary that strict accountability be maintained at all times. The National Computer Center maintains a computer inventory list for this purpose which included all reels at the Center. However, under current procedures, the Center cannot prepare an inventory of tapes by location such as the tape library, storage vault, etc. Thus, when a search for a tape is made, all possible locations must be checked until the tape is located. Such a system does not permit positive control over magnetic tapes as evidenced by the Center's May 1975 physical inventory which disclosed 33 missing reels.

In addition, we found that tape library operations at some of the service centers were deficient. Computer branch personnel had virtually unlimited access to the tape library and the library was not locked on the weekends when the librarians were not on duty. In a test of tape library controls at the Covington Service Center, we found that tapes could be removed with little or no possibility of detection. Further,

inventories on magnetic tapes in the library were not conducted on a semiannual basis as required by the Library Operations Handbook. For example, the Chamblee Service Center did not inventory tapes between December 1972 and July 1974.

Selected information from each taxpayer's return is converted to microfilm at the National Computer Center and furnished to the service centers for their use. Additional copies of the microfilm are produced at the service centers according to need. Appropriate procedures have not been implemented to account fully for the microfilm cartridges at all service centers.

We conducted an inventory of microfilm cartridges in the input perfection branch of the Covington Service Center and compared our count with the records maintained by the branch. The results were as follows:

Category	GAO	IRS
Business Master File	735	738
Individual Master File	2,691	2,802
Federal Tax Deposits	256	127
Residual Master File	21	21
Total	3,703	3,688

An examination by IRS disclosed errors in the records that accounted for the discrepancies between the totals but did not resolve the discrepancies within categories. The differences in the category may have been due to misclassification, but it is indicative of poor accounting procedures. Further, the number of cartridges that should have been on hand within the input perfection branch could not be independently verified by reference to records other than those of the branch. This was because no master record was maintained by the center of the microfilm cartridges reproduced, distributed, and destroyed.

CONCLUSION

The controls for document and information flow were considered generally adequate to insure the proper processing of tax returns and related documents and should be continued under TAS. However, improvements are needed in the areas of personnel screening and information storage.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

We recommend that IRS:

--Consider ways and means to protect taxpayer data from improper access by non-IRS employees having access to a facility where taxpayer information is maintained. This would include contractual provisions requiring either appropriate background investigations or escort service to non-IRS employees without a current background investigation.

--Require mandatory periodic updating of personnel investigations.

--Initiate procedures to provide appropriate accountability and control of all magnetic tapes, microfilms, and other information media.

AGENCY COMMENTS AND ACTIONS

The Commissioner of Internal Revenue expressed the Service's concern about protection of taxpayer data from improper access by non-IRS employees working in the data processing facilities. With regard to appropriate background investigations on these individuals, the Commissioner is requesting advice from the IRS chief counsel. If the Service has statutory authority, it will determine the type of investigations that are appropriate, based on the degree to which non-IRS employees have access and other risk factors, as well as the cost of conducting the investigations. He further stated that internal controls which limit the access and movement of non-IRS employees are presently prescribed, including a mandatory provision for escorting all nonfederal personnel in restricted areas. A small number of nonfederal personnel who have a clearance of confidential or higher, issued under auspices of the Defense Industrial Security program, are allowed unescorted access to some restricted areas. The use of escorts in nonrestricted areas is left to the discretion of the center directors. The adequacy of these safeguards is being measured by ongoing security tests performed by the organizational elements under IRS Assistant Commissioner for inspection.

The Commissioner agreed that background investigations of some IRS employees who use or have access to taxpayer information should be updated periodically. The Service is studying which positions require full-scale investigations due to their sensitivity.

The Commissioner indicated that the IRS internal auditors had also noted weaknesses in the accountability and control of information and stated that the Service had taken specific corrective action which included issuance of revised procedures providing for tighter controls on magnetic tapes, discs, and printouts as well as on access to tape libraries.

CHAPTER 5

PHYSICAL PROTECTION OF IRS COMPUTER FACILITIES

Physical protection of an automated data processing facility involves permitting access to the facility by authorized individuals while denying access to others. In order to accomplish this objective, Internal Revenue Service computer facilities are equipped with electronic intrusion detection devices, silent trouble alarms, and related industrial protection systems, that are monitored at protection consoles. All but one of the service centers have a perimeter security fence. Guard services are either furnished by the General Services Administration or on a contract basis. Exterior security lighting is provided for buildings, parking lots, and the perimeter fence.

Within the data processing facilities, physical security of tax data is further provided by a system of restricted and secured areas as part of the IRS physical and document security program. Access to a facility and the designated restricted areas is controlled through the use of a personnel identification system. Under this system color coded photograph badges are used to control the movement of IRS personnel, contract support personnel, and visitors. The system is intended to limit access to those persons who have need to enter a given area in the performance of their duties.

We consider the above physical protective measures employed by the Service to be generally adequate in safeguarding their computer facilities. However, the effectiveness of the measures has been diminished by a lack of proper implementation and maintenance. This chapter discusses those areas where improvements are considered necessary in order to meet the overall physical security objective.

In addition to the physical safeguards covered by this review, special procedures relating to the transportation, storage, and disposal of IRS records, including tax returns, have been developed jointly with the National Archives and Records Service of the General Services Administration and the U.S. Postal Service.

PERIMETER PROTECTION

IRS' perimeter protection at its computer facilities is designed to deter trespassing and to direct employees and

visitors to selected entrances. Our examination of the physical protection features used disclosed the following deficiencies resulting from improper maintenance.

Perimeter fencing at the Brookhaven Service Center was in need of repair and strengthening. Spaces under fencing existed that would permit unauthorized access and numerous areas were found where barbed wire strands at the top of the fence were broken. In addition, locks to perimeter doors of the Center had not been changed since the facility was opened in October 1972. While officials said that there was no requirement to periodically change locks on access doors, we believe that good security practices necessitate such actions. This procedure would help maintain an appropriate level of facility protection when the employees given access to perimeter door keys are changed.

It is essential that IRS provide for the continuous inspection and maintenance of protective devices to insure that they fulfill their intended purpose. Improper maintenance can significantly reduce their effectiveness and impede the overall security of the facility.

ACCES CONTROLS

Access to computer facilities is controlled through use of identification badges. Employees must show their badges to a security guard upon entering and display them at all times in the facility. Visitors are issued badges and generally require escort by IRS personnel.

Certain critical areas within each service center have been designated as "restricted" with access limited to authorized individuals. Access to a restricted area is controlled through use of identification badges that are distinctive in color. For example, the normal badge for an IRS employee may be yellow, a visitor's red, and a restricted area badge such as the computer room may be brown.

The effectiveness of the badge control system is dependent upon the willingness of security guards and IRS employees to challenge any individual not displaying a proper identification badge while in the facility. Further, it is necessary that all badges be properly accounted for and controlled as they not only represent the principal means of identification but under TAS will be used as one step in activating computer terminals.

In a test of the badge system at the Covington Service Center, access was gained to several restricted areas while displaying a "visitor's escort only" badge. Such a badge did not authorize access to any of the restricted areas within the Center. During a further test, movement was permitted unchallenged without badge or escort through many of the Center's work areas.

Administrative controls over employee and visitor identification badges were ineffective at both the Brookhaven and Chamblee Service Centers. Lost or missing badges were not always accounted for, and reconciliations were not made as required. Procedures were generally inadequate to insure that badges were collected upon furlough or termination of employment. For example at the Chamblee Service Center, badges had not been returned to the badge unit by mid-June for 110 temporary employees whose employment was terminated on May 11, 1975. In seven instances, former employees were permitted to clear the Center without surrendering their identification badges. The remaining 103 badges were being held in the branches where the former employees had worked.

No form of disciplinary action was taken where employees of the Brookhaven Service Center repeatedly forgot or lost their identification badges. An IRS official estimated that approximately 15 to 20 badges were lost and 400 instances of forgotten badges occurred each month. Such laxity in the administration of the badge control system has, in our opinion, significantly weakened the overall security of the service center.

PHYSICAL CONTROL OVER TRASH DISPOSAL

Large quantities of waste material containing taxpayer information must be disposed of daily and therefore must be protected to prevent disclosure; within IRS, this is accomplished in various ways. In general, trash containing taxpayer information is segregated and destroyed by incinerating, pulping, shredding, or otherwise disintegrating the material. The destruction is accomplished by IRS or by contract under IRS supervision.

While the above process would appear to provide adequate protection, a basic weakness exists. The effectiveness of the safeguard depends on the individual IRS employee properly segregating trash containing taxpayer information from nonsensitive waste. During our review at the Covington Service Center, taxpayer information was found in general use wastebaskets and trash containers. At the National Computer Center,

taxpayer information was found exposed at a sanitary landfill. These findings point to a need to review the disposal process and to consider requiring all trash to be destroyed in the same manner, thus eliminating the segregation process.

CONCLUSION

The physical protection measures and procedures employed by IRS are considered adequate, in concept, to properly protect taxpayer data maintained by IRS ADP facilities. However, the lack of proper implementation and application has resulted in several of the controls being less than effective. These conditions should be corrected in the present system and the controls continued in TAS.

RECOMMENDATION TO THE COMMISSIONER OF INTERNAL REVENUE

We recommend that the national office exercise responsibility for periodically evaluating the effectiveness of physical security at each of the 10 service centers and the National Computer Center. While all aspects of physical protection should be evaluated, particular attention should be given to correcting the discrepancies cited herein with emphasis on obtaining proper implementation of effective badge control and trash disposal systems. The results of the evaluations should be analyzed and where warranted, uniform procedures should be developed for application at all locations and continued under TAS.

AGENCY COMMENTS AND ACTIONS

The Commissioner of Internal Revenue informed us that plans are now being made to increase evaluations of physical security and to conduct them on a systematic, regular basis. He stated that protective programs branch has responsibility for this program but has been unable to make frequent evaluations because of their small staff. Independent tests will continue by the organizational elements under the Assistant Commissioner for Inspection.

According to the Commissioner, corrective action has been initiated regarding those protective measures which are prescribed but not effective because of lack of proper maintenance or implementation. The Service had studied its trash disposal procedures and had issued new Service-wide guidelines which will require all trash to be processed in the same manner and should overcome the deficiencies noted during our review. He further stated that administrative control over badges in

certain service centers should improve with the recent assignment of new security officers who will receive strong management support in the administration of the badge system. The Service is testing a new photograph badge with computer readable encoding which, if successful, will replace the present badge system which relies on visual checks by guards and IRS employees.

CHAPTER 6

NETWORK SECURITY AND INTERSERVICE CENTER ACTIVITY

The proposed Tax Administration System is envisioned as a totally integrated data system involving processing, storage, data communications, and terminal facilities. A decentralized data base will be used and each service center will process and maintain tax accounts for taxpayers in its geographic area. The National Communications Center will control data exchange between centers and will maintain a directory of each center's records so that a taxpayer's account will not be maintained at more than one center.

Data communications will be provided by a data communication subsystem. This subsystem will link the data terminals located in field offices with the host service center. Service centers will be interconnected through the National Communications Center. Information that must be transferred between service centers will be batch processed to the National Communications Center for relay to the appropriate service center. Data will be transmitted between centers and the National Communication Center over encrypted data links. Through this design, a local office terminal will communicate only with its servicing center, and no direct terminal-to-terminal or center-to-center communications will take place.

Encryption of the data links and the batch transfer of data were recommended by the Office of Management and Budget and cited by IRS as data communication safeguards in their notification of proposed system changes required by the Privacy Act of 1974 and submitted to the Congress and the Office of Management and Budget on October 15, 1975.

DATA ENCRYPTION

The GAO report entitled, "Computer-Related Crimes in Federal Programs" (FGMSD-76-27, Apr. 27, 1976), observed 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. While wiretapping and electronic interception of communications are technically possible, the extent of the threat to taxpayer data from such sources has not been established. For example, our discussions with the Federal criminal and intelligence agencies and with IRS have disclosed no known cases of

unauthorized disclosure of taxpayer information traceable to data communications.

When a risk and threat analysis indicates the necessity for safeguarding the communication links, cryptography can be used to secure the network. An algorithm that satisfies the primary technical requirements of a data encryption standard was published in the Federal Register of March 17, 1975, by the National Bureau of Standards. This algorithm is to be used by Federal agencies where encryption of data communications is considered necessary. However, the National Bureau of Standards recommends that other security safeguards such as identification, access control, and access auditing be implemented before sophisticated encryption devices are procured for the protection of personal data. The devices employing the algorithm are not generally available and their cost has been estimated to range from a few hundred to several thousand dollars.

For planning purposes, IRS is considering the unit cost of the encryption devices to be approximately $2,500 with an equal amount representing maintenance cost over a 10-year system life. Forty-two devices will be required to provide partial network protection representing the data communications between the service centers and the National Communications Center. Eight hundred ninety-three additional devices would be required to provide encryption between the field office terminal control units and the service centers. Full end-to-end encryption at each field terminal would require approximately 3,350 devices 1/ to secure the network. The estimated incremental cost of encrypting the IRS data communications network is shown in the following chart.

1/Of the approximately 8,000 terminals to be connected to the system, about 2,900 will be located outside the 10 IRS service centers and will require use of commercial communications. Devices for encryption/decryption would be required at each of these terminals and others would be necessary at the various service centers to provide for full end-to-end encryption.

Estimated Cost of Encryption of IRS Data Communication Network

Estimated cost of encryption devices	Partial protection	Intermediate protection	Full protection
	(000 omitted)		
Between service centers and National Communications Center	$105	$ 105	$ 105
Between field office terminal control units and host service center	-	2,233	-
Between field office data terminals and host service centers	-	-	8,375
Total estimated equipment cost	105	2,338	8,480
Total estimated maintenance cost	105	2,338	8,480
Total estimated cost	$210	$4,676	$16,960

Although we recognize that a potential for wiretapping or electronic interception exists, our inquiries disclosed no evidence of a present threat to taxpayer information that would warrant the cost of procuring encryption devices to secure the communication network. A risk and threat analysis has been initiated by IRS and its completion is considered necessary prior to any decision to employ this technology.

BATCH TRANSFER OF DATA

Under TAS, data is to be transmitted over high-speed communication lines from a service center to the National Communications center for processing or relaying to another service center in batch form. These procedures preclude direct communication between the computers located at the service centers.

While prohibiting realtime interservice center activity may be desirable for economy or other considerations, it does not provide communications security and does not significantly add to the overall security of TAS. This is due to the fact

that batch processing delays, but does not control, the transfer of data. For example, the delay may discourage, but will not prevent, an IRS employee at one location from browsing the tax information maintained at another service center.

Interservice center activity should be controlled at the source through supervisory intervention. This would require a supervisor to validate all requests for taxpayer information maintained by another service center. While a manual review and approval of requests as currently planned by IRS would provide a degree of control, such a procedure could be circumvented. Automation of the validation process would, in our opinion, provide the most effective control to prevent unauthorized transfer of data between centers. A supervisor would be required to enter into a terminal, validation data that would release each individual request. Such a process would preclude an employee from obtaining taxpayer information from another center without independent confirmation as to need.

CONCLUSION

The internal threat to taxpayer information from unauthorized use of the communication network is considered greater than the external threat posed by covert electronic interception. Therefore, the need to control interservice center activity is evident while the need to encrypt the communication links has not been established.

RECOMMENDATION TO THE COMMISSIONER OF INTERNAL REVENUE

We recommend that appropriate controls be established in the design and implementation of TAS to insure that only authorized transfers of taxpayer information between centers are permitted. Further, the need to provide sophisticated communication security should be subjected to a thorough risk and threat analysis prior to any decision to incure the cost for encryption devices.

AGENCY COMMENTS AND ACTIONS

The Commissioner of Internal Revenue informed us that IRS was carefully considering the recommendation concerning a requirement for supervisory terminal validations and counter authorization for data that was accessed, based on geographic areas or levels of account activity. The Commissioner stated that a need may exist for certain exceptions in applying geographic restraints.

The Commissioner also stated that the Service was developing a risk analysis to reevaluate the need for communication line encryption devices prior to any contract award and, if not fully justified, would re-examine the issue with the Office of Management and Budget.

CHAPTER 7

THE IRS SECURITY PROGRAM

The IRS national office has the overall responsibility for the formulation and implementation of the security program. Policy responsibility has been assigned to the Internal Revenue Service Security Council. The Council is chaired by the Assistant Commissioner for Administration with five additional Assistant Commissioners serving as members. The chief of the protective programs branch of the facilities management division has been designated executive secretary.

IRS regulations direct the Council to deal with all security issues within IRS. The Council is authorized to assess security status, identify important issues and problems, and determine which items are to be referred to the Deputy Commissioner or Commissioner for final decision. The Council has the authority to obtain the expertise necessary to deal with any and all security issues. It can also recommend methods for evaluating security to insure that prescribed policies and procedures are being followed. Similar councils exist at several regional offices and service centers.

The facilities management division, through its protective programs branch, oversees the Service-wide implementation of the physical and document security program at the national level. Its counterparts at the National Computer Center and the service center protective programs offices are responsible for developing and carrying out the program within their respective areas of responsibility.

Similar responsibility for data processing security has not been defined. At the national level, there is no single office or organizational element responsible for the overall implementation of the technical security measures that are necessary and integral to the data processing operations and programs. Each data processing project or operational function considers only those controls and security measures related to its system or subsystem. Such an organizational approach to security does not insure uniform implementation of the security policies established by the Internal Revenue Service Security Council.

A security administrator is assigned to each of the IRS service centers. However, their area of responsibility has been limited to the Integrated Data Retrieval System, a subsystem of a center's operation. Overall responsibility for data processing security has not been vested in an individual or office at the local level.

CONCLUSION

Establishing an organizational structure to independently monitor and evaluate data processing security would, in our opinion, significantly contribute to overcoming the weaknesses in controls cited in this report. Responsibility and authority must be clearly defined and a continuing program established to insure that taxpayer data is properly safeguarded in accordance with the Privacy Act of 1974.

RECOMMENDATION

We recommend that the Commissioner of Internal Revenue establish a national data processing security office responsible for technical, administrative, and physical security to include all data processing facilities. Such an office should be independent of those organizational elements responsible for the development and operation of the computer systems and facilities and have authority sufficient to assure appropriate security.

A similar position should be established at each data processing facility. The data processing security officer should be independent of day-to-day line operations. Such independence can be achieved by either making this position a field extension of the national office or placing it under the head of the facility with direct communication authorized with the national data processing security office.

AGENCY COMMENTS AND ACTIONS

The Commissioner of Internal Revenue stated that IRS recognized the merits of this proposal and that a study would be initiated to thoroughly evaluate the national security office concept and determine its organizational and resource implications.

CHAPTER 8

OBSERVATIONS AND MATTERS FOR CONSIDERATION BY THE CONGRESS

OBSERVATIONS

A widespread concern has often been expressed about the theory that large computer projects could be expanded and linked to other computer systems and thus pose a serious threat to the privacy of the individuals involved in various Government operations or programs. The first attempt to centralize Government-held computerized information was made in the mid-1960s with the proposal to establish a National Data Center. This proposal met with concern over the potential misuse of a large concentration of data accumulated from the various Federal agencies which could result in an invasion of individual privacy.

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

More recently, the Joint Agriculture-GSA New Equipment Project (commonly known as FEDNET) met similar opposition. As a result, the scope of the project was reduced in July 1974 by canceling the telecommunications network and GSA participation in the project. Agriculture canceled its procurement action in October 1975.

IRS' proposed Tax Administration System differs significantly from the National Data Center and FEDNET concepts in that direct linkage, or sharing of equipment, with other agencies is not involved. Further, TAS provides for the decentralization of the data base in contrast to the consolidation of information as was proposed for the National Data Center.

1/House Committee on Government Operations Report, "Privacy and the National Data Center Concept," 90th Congress, 2nd sess., House Report No. 1842, (1968), p. 8.

Under the current IRS computer system, the Service sends and receives data by way of magnetic tapes to other organizations to facilitate tax administration. This practice will continue under TAS. The following are examples of such indirect interfaces with other computer systems.

--The Service receives a substantial portion of the data concerning interest and dividends paid by business taxpayers (as required by sections 6041 and 6042, Internal Revenue Code of 1954) on magnetic tapes, thereby permitting the matching of such data with its master file accounts and avoiding the expense of transcribing and converting it to machine readable form.

--Magnetic tapes received from the Social Security Administration are used to verify the social security numbers required by section 6109, Internal Revenue Code of 1954, to be furnished on individual income tax returns. Such verification helps to assure the accuracy of the master file accounts.

--The Service extracts self-employment income data and sends this information by way of magnetic tapes to the Social Security Administration so that agency can credit the individuals' social security accounts as provided in 42 U.S.C. 401.

--The Service sends data, which is authorized by section 6103 of the Internal Revenue Code of 1954, on magnetic tapes to other Government agencies such as the Bureau of Census for statistical purposes, and to various states to assist in the tax administration of their residents.

CONCLUSIONS AND MATTERS FOR CONSIDERATION BY THE HOUSE AND SENATE COMMITTEES ON APPROPRIATIONS

It is our opinion that as the user population of tax information expands, the risk of unauthorized disclosure also increases. Therefore, we believe the Congress may wish to consider certain restrictions in any legislation authorizing or funding the development and implementation of TAS. Such legislative restrictions would involve (1) direct linkage between TAS and any other computer systems, (2) location of TAS input and output devices, and (3) interface of TAS with other systems.

Although the current IRS computer system is not directly linked with any other system and such linkage has not been included in any TAS planning document we examined, we believe the Congress may wish to consider making such direct linkage unlawful.

Another prohibition that could be considered is to preclude a computer terminal, or other input or output devices with direct access to the tax account data base, from being located at other than IRS operating locations unless specifically authorized by law.

The Service currently receives data on computer media such as magnetic tapes, from the public and private sectors to facilitate tax administration. It sends data via computer media to other Government agencies and to various States as authorized by law, resulting in a cost savings to both the Government and the taxpayer. The Congress may wish to consider legislation restricting the use of such indirect interfaces for new purposes unless specifically authorized by statute.

CHAPTER 9

SCOPE OF REVIEW

This report provides our assessment of the proposed Tax Administration System's capability to provide appropriate safeguards to protect taxpayer information as required by the Internal Revenue Code and the Privacy Act of 1974. A separate report is being issued on our evaluation of the reasonableness of the cost/benefit analysis for the proposed new system.

We interviewed IRS officials and examined records and documents pertaining to the proposed Tax Administration System. We evaluated selected technical, administrative, and physical safeguards currently in the present system which are planned to be retained in TAS. We plan to continue our assessment of the privacy and security aspects of the current system and may issue future reports if appropriate.

Section 6103 of the Internal Revenue Code of 1954 authorizes certain Government officials, Federal agencies, and the States access to taxpayer information maintained by IRS. We did not review the safeguards on the taxpayer information provided those recipients since that access is authorized by law and has no impact on the ability of TAS to safeguard taxpayer information. However, those officials and agencies with statutory authority to gain access to taxpayer information are required to safeguard that information against unauthorized or inappropriate disclosure. In addition, the Commissioner of Internal Revenue has stated that he will require a review of the agreements with the States and renegotiate those that do not provide adequate safeguards for taxpayer information.

We conducted our review at the IRS (1) national office in Washington, D.C., (2) National Computer Center at Martinsburg, West Virginia, (3) Cincinnati, Ohio, district office, and (4) service centers in Chamblee, Georgia; Brookhaven, New York; and Covington, Kentucky.

APPENDIX I

Department of the Treasury / **Internal Revenue Service** / Washington, D.C. 20224

Commissioner

JUL 16 1976

Mr. Victor L. Lowe
Director, General Government Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Lowe:

We appreciate the comprehensive review made by your staff of the Internal Revenue Service's present automatic data processing system and the proposed Tax Administration System (TAS). We found the periodic briefings and open discussions which you arranged throughout the audit to be particularly helpful. The on-line approach gave us an opportunity to take early corrective action where needed within the existing security system; and it allowed us to release (with your consent) GAO's overall favorable conclusion to those in the TAS clearance process.

Our comments on your recommendations listed on pages iii and iv in the draft report, "Evaluation of the Ability of the Internal Revenue Service's Proposed Computer System to Safeguard Taxpayer Information," are contained in ATTACHMENT A to this letter. We noted several editorial changes which you may wish to consider also. These are cited in ATTACHMENT B. Remedial actions have been or are being taken in those areas which can be corrected within the framework of the existing security procedures, methods or controls. However, a few recommendations will require further study.

As stated in your recent report concerning the adequacy of physical security and risk management policies and practices (FGMSD-76-40), "Perfect security is generally regarded as unattainable; therefore, the aim of a good physical security system should be to reduce the probability of loss to an acceptable low level at reasonable cost and to insure adequate recovery in case of loss." We strongly endorse this concept. You may be assured that as the TAS design effort continues and implementation takes place, every effort will be made to provide the highest reasonable level of security and protection for taxpayer information, and that all of the recommendations made by the GAO will be carefully considered.

With kind regards,

Sincerely,

Commissioner

Attachments

ATTACHMENT A

Responses to GAO's Recommendations to the Commissioner

1. "Establish a national data processing security office and a similar position at each data processing facility responsible for administrative, physical and technical security."

We recognize the merits of this proposal; and, therefore, a study will be initiated to thoroughly evaluate the national security office concept and determine its' organizational and resource implications.

2. "Consider ways and means to protect taxpayer data from improper access by non-IRS employees having access to a facility where taxpayer information is maintained."

The Service is concerned about protection of taxpayer data from improper access by non-IRS employees working in our data processing facilities. With regard to appropriate background investigations on these individuals, we are requesting advice from the IRS Chief Counsel on Service authority and investigative jurisdiction. If the Service has statutory authority, we will determine the type of investigations that are appropriate, based on the degree to which non-IRS employees have access and other risk factors, as well as the cost of conducting the investigations. Internal controls which limit the access and movement of non-IRS employees are presently prescribed, including a mandatory provision for escorting all non-Federal personnel in restricted areas. A small number of non-Federal personnel who have a clearance of confidential or higher, issued under auspices of the Defense Industrial Security Program, are allowed unescorted access to some restricted areas. The use of escorts in non-restricted areas is left to the discretion of the center directors. The adequacy of these safeguards is being measured by Inspection's on-going security tests.

3. "Require mandatory periodic updating of background investigations of employees using or having access to taxpayer information to ensure that their activities warrant the Government's continued trust."

We agree that the background investigations of some IRS employees who use or have access to taxpayer information should be updated periodically. Presently, we are studying which positions require full scale investigations due to their sensitivity, and we believe once these are clearly identified we can analyze and reach a final conclusion regarding your recommendation.

4. "Initiate procedures to provide appropriate accountability and control of all magnetic tapes, microfilms, and other information media."

Our internal auditors have also indicated that weaknesses exist in this area. We have taken specific corrective action which includes the issuance of revised procedures (Revision to Handbook 12010, Security) providing for tighter controls on magnetic tapes, discs and print-outs as well as access to tape libraries. As you suggested, we have studied our trash disposal procedures. This study was extended to include all offices and has resulted in Service-wide guidelines.

APPENDIX I

5. "Require periodic evaluations of the effectiveness of physical security at each service center and the National Computer Center."

Plans are now being made to increase such evaluations and to conduct them on a systematic, regular basis. Our Protective Programs Branch, which has responsibility for this program, has been unable to make frequent evaluations because of their small staff. Independent tests by Inspection will continue.

Corrective action has been initiated with regard to those protective measures which are prescribed, but were not effective because of lack of proper maintenance or implementation. Problems in administrative control over badges in certain service centers should be corrected by the recent assignment of new security officers who will receive strong management support in the administration of the badge system. Furthermore, the Service is testing a new photograph badge with computer readable encoding. If successful, it will replace the present badge system which relies on visual checks by guards and IRS employees.

6. & 7. "Eliminate listings of employee access identification data where possible and employ one-way encryption to safeguard data files containing such information."

"Provide additional restrictions on terminal users of the automatic data processing system to permit access only to those functions and related data that are necessary to perform their duties."

As a result of Inspection's internal audit findings and your recommendations, we have eliminated the listings of employee access identification data, and we are encrypting employee access identification data as a further safeguard. Also, we have taken steps to automate the assignment and deletion of command codes assigned to terminal operators. Specifically, when employees are transferred to new functional units, their previous command codes are deleted, and the new codes necessary to perform their new duties are generated upon input of a proper "key" command code.

We believe these measures which have already been implemented substantially strengthen our system safeguards. The sophisticated techniques of fully automating the password generation, assignment and distribution process, and "one-way" encryption of all access data and files is being explored for possible use in the future.

8. "Initiate controls over the activities of those employees that have technical training necessary to circumvent security safeguards."

We recognize the vulnerability of the ADP system in this area. Thus, consideration is being given to various methods and procedures to control the activities of technical employees, particularly resident programmer analysts, and balance security concerns with the need for employee efficiency.

APPENDIX I

9. "Seek legal authority to withhold from public disclosure data processing documentation that would substantially enhance the ability to gain illegal access to taxpayer information."

As a result of discussions with GAO auditors, a comprehensive review of ADP documentation is in process to identify materials which, for security reasons, should not be publicly disclosed. If the Service finds that current exemptions of the Freedom of Information Act do not offer sufficient protection to sensitive ADP systems material, appropriate legislation will be sought.

10. & 11. "Establish appropriate controls to ensure that only authorized inter-service center activity is permitted."

"Require supervisory approval for all out-of-district inquiries to taxpayer accounts by taxpayer compliance employees and to inactive accounts by taxpayer service representatives."

We agree with the principle implied in these recommendations that terminal users should not have access to more tax account data than is necessary to perform their assigned duties. Thus, as you recommended, we have initiated a study to thoroughly explore all aspects of this important subject. The objective of the study is to identify practical ways to limit access to data without adversely affecting service to the public or productivity of the terminal users or their supervisors. In addition, we will continue to evaluate the use of additional positive identifiers of terminal users (beyond badge, password, and employee profile controls).

We are carefully considering your recommendation concerning a requirement for supervisory terminal validations and counter authorization for accesses based on geographical areas or levels of account activity. Our initial review indicates that we may be able to use the account linkage data as a control aid. On the other hand, a need may exist for certain exceptions in applying geographical restraints.

12. "Insure that communication risks and threats are completely analyzed prior to any decision to incur the cost for sophisticated security devices."

The Service is developing a risk analysis to reevaluate the need for communication line encryption devices prior to any contract award. If such equipment is not fully justified, the Service will re-examine the issue with the Office of Management and Budget (OMB).

PRINCIPAL OFFICIALS RESPONSIBLE FOR ADMINISTRATION OF ACTIVITIES DISCUSSED IN THIS REPORT

	Tenure of office From	To
SECRETARY OF THE TREASURY:		
William E. Simon	Apr. 1974	Present
George P. Shultz	June 1972	Apr. 1974
COMMISSIONER OF INTERNAL REVENUE:		
Donald C. Alexander	May 1973	Present
ASSISTANT COMMISSIONER, ACCOUNTS, COLLECTION, AND TAXPAYER SERVICE:		
James I. Owens (acting)	Aug. 1976	Present
Robert H. Terry	Aug. 1973	July 1976
ASSISTANT COMMISSIONER, PLANNING AND RESEARCH:		
Anita F. Alpern	Jan. 1975	Present
Dean J. Barron	Aug. 1973	Dec. 1974
DIRECTOR, TAX SYSTEMS REDESIGN DIVISION:		
Patrick J. Ruttle	Dec. 1975	Mar. 1976
Donald G. Elsberry	Nov. 1973	Dec. 1975
DIRECTOR, TAX ADMINISTRATION SYSTEMS DIVISION:		
Patrick J. Ruttle	Mar. 1976	Present

Note: In March 1976, the responsibility for TAS was transferred from the Office of the Assistant Commissioner (Planning and Research) to the Assistant Commissioner (Accounts, Collection, and Taxpayer Service). With the transfer, the Tax Systems Redesign Division was abolished and the Tax Administration Systems Division established.