DOCUMENT RESUME

02800 - [A2153252]

IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information. GGD-77-44; B-137762. Jujy 11, 1977. 70 pp. + 2 appendices (15 pp.).

Report to Chairman and Vice Chairman, Joint Committee on Taxation; by Elmer B. Staats, Comptroller General.

Issue Area: Tax Administration (2700).
Contact: General Government Div.
Budget Function: General Government: Other General Government (806).
Organization Concerned: Internal Revenue Service.
Congressional Relevance: House Committee on Ways and Means; Senate Committee on Finance; Joint Committee on Taxation.
Authority: Tax Reform Act of 1976. Privacy Act of 1974.

The Internal Revenue Service (IRS) designed a security program to protect the confidentiality of tax data under its control, but weaknesses in carrying out the program are widespread, and some essential procedures and controls are totally lacking. Findings/Conclusions: Inadequate controls over computer operations afforded many opportunities for IRS employees and others to unlawfully disclose tax data. Computer programmers could easily run an unauthorized program or make an unauthorized program change without detection. Controls were exercised inadequately over IRS' primary computerized data retrieval system. Employees were able to get unneeded tax data because IRS was not enforcing its policy of limiting employee access to only the data needed to perform official duties. IRS employees were also able to get unneeded tax data due to equipment shortages. There is potential for unauthorized tax data disclosure due to IRS' methods for assessing the integrity of employees and others having access to its facilities. Although facility physical features and guard service were adequate to deter general access by unauthorized persons to IRS facilities, other aspects of physical security were weak and precluded maximum protection of tax data. Thirty-two recommendations designed to correct specific weaknesses were made by GAO. IRS agreed with most of the recommendations. (Author/SC)

REPORT TO THE JOINT COMMITTEE ON TAXATION
CONGRESS OF THE UNITED STATES

BY THE COMPTROLLER GENERAL
OF THE UNITED STATES

IRS' Security Program Requires Improvements To Protect Confidentiality Of Income Tax Information

Department of the Treasury

IRS designed a security program to protect the confidentiality of tax data under its control. But weaknesses in carrying out the program are widespread and some essential procedures and controls are lacking completely. Because of the program shortcomings, an untrustworthy employee or others having access to IRS facilities could penetrate the safeguards and obtain unauthorized tax data with little chance of detection. GAO made 33 recommendations to strengthen the security system. IRS agreed with most of them.

GGD-77-44

JULY 11, 1977

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

B-137762

To the Chairman and Vice Chairman
Joint Committee on Taxation
Congress of the United States

This report, one of a series in response to your Committee's request, addresses the Internal Revenue Service's security program and related improvements required to protect tax data confidentiality. The Service agreed to most of our recommendations and effective implementation of them should result in a sound security program to protect tax information.

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

Elmer B. Staats

Comptroller General
of the United States

COMPTROLLER GENERAL'S REPORT
TO THE JOINT COMMITTEE ON
TAXATION
CONGRESS OF THE UNITED STATES

IRS' SECURITY PROGRAM REQUIRES IMPROVEMENTS TO PROTECT CONFIDENTIALITY OF INCOME TAX INFORMATION
Department of the Treasury

DIGEST

The need for preserving the confidentiality of income tax returns and tax information is a strongly held and often expressed public concern. Accordingly, the Congress has passed laws requiring the Internal Revenue Service (IRS) to protect the confidentiality of taxpayer data under its control and providing penalties for unauthorized disclosure of tax data.

In a January 1977 report, GAO evaluated the ability of IRS' proposed computerized tax administration system to protect taxpayer information adequately. GAO stated that with proper design and implementation, the system could provide a high level of protection. That report also commented on certain weaknesses in the existing system for safeguarding tax data confidentiality.

This report continues, in greater detail, the discussion of weaknesses in the existing system.

Collections of tax data are widespread and not restricted to IRS. Tax data is held by States, professional and commercial tax practitioners and by taxpayers themselves. Obviously, IRS cannot protect the confidentiality of tax data held by these sources.

But what about tax information under IRS control? IRS' security program does not assure confidentiality. Its security safeguards could easily be penetrated--especially by IRS employees and others having access to the facilities. Such individuals could obtain access to tax returns or income tax data on a large, random number of taxpayers with little chance of detection. Employees,

Tear Sheet. Upon removal, the report cover date should be noted hereon.

depending on the position occupied, could make unauthorized access to tax data on preselected taxpayers. (See p. 9.)

Nevertheless, known unlawful disclosures have been relatively few. In 1976, IRS investigated 182 allegations of unauthorized disclosure and identified responsibility for 43. (See p. 6.) But the relatively small number of known unauthorized disclosures was not due to a lack of opportunity.

IRS has a vast amount of tax information and thousands of employees whose duties require access to at least some of it. Limiting access to those having a genuine need is a sizable problem. While IRS designed a security program to limit access, it relies more heavily on the integrity of its employees and others than on strict enforcement of prescribed security measures.

Fragmented responsibility is the principal cause of IRS' weakness in assuring adherence to its security regulations. Security program responsibility is assigned to four organizations each having responsibility for other major IRS functions. In most instances, the other functions quite naturally are given priority over security matters. IRS employees' concern and awareness of tax data confidentiality would improve if security responsibility were centralized in one office. (See pp. 10 and 11.)

Accordingly, GAO recommends that the Commissioner of Internal Revenue establish a separate office with sufficient independence and authority to develop security procedures and to monitor day-to-day compliance with all facets of the security program at all IRS facilities. (See p. 11.) IRS agreed with GAO's recommendation.

SPECIFIC SECURITY WEAKNESSES

Inadequate controls over computer operations afforded many opportunities for IRS employees and others to disclose tax data unlawfully. Computer programmers could easily run an unauthorized program or make an unauthorized program change without detection. Magnetic tapes, each containing tax data on as many as 5,000 taxpayers, were not properly controlled and some could not be accounted for. Computer printed products also were not controlled so that IRS could be sure that they were received only by authorized persons. (See p. 12.)

Controls were exercised inadequately over IRS' primary computerized data retrieval system. The system includes 4,000 terminals which enable about 18,600 authorized users to have instantaneous access to many taxpayer accounts. Many users can access data on any taxpayer except those few whose accounts IRS has restricted. Service center users had use of system codes allowing access to data they did not need. Tapes containing system security information and manuals describing the built-in system security features were not secured adequately. (See pp. 25 and 30.)

Employees were able to get unneeded tax data because IRS was not enforcing its policy of limiting employee access to only that data needed to perform official duties. For example:

--Some IRS installations permitted almost wholesale entry to restricted areas containing sensitive tax data. (See p. 39.)

--Some IRS supervisors were not reviewing tax data requests or spot checking the data obtained to determine whether the requester officially needed it. (See p. 40.)

IRS employees were also able to get unneeded tax data due to equipment shortcomings. The equipment used to make microfilm transcripts cannot print data on just one taxpayer. For example, a test of 134 microfilm transcript requests showed that the transcripts contained unneeded tax data on 2,197 other taxpayers. (See pp. 41 and 42.)

There is also potential for unauthorized tax data disclosure due to IRS' methods for assessing the integrity of employees and others having access to its facilities. IRS placed some employees in sensitive positions before obtaining required reports on their backgrounds and allowed some guards and janitors into restricted areas without knowing whether background checks had been made. (See pp. 46, 50, and 51.)

Although facility physical features and guard service were adequate to deter general access by unauthorized persons to IRS facilities, other aspects of physical security were weak and precluded maximum protection of tax data. For example:

--Tax data was readily accessible to or in plain view of guards and janitors during IRS off-duty hours. (See p. 60.)

--Senders of tax data were not following up by obtaining acknowledgment receipts. (See p. 62.)

--Periodic inventories of microfilm were not being taken. (See p. 63.)

--Security personnel were not checking on the physical security system. (See p. 61.)

Security of tax data at Federal Records Centers generally was adequate. But janitors, guards, General Service Administration maintenance personnel, and others were permitted unescorted access to the tax return storage area. Another security weakness was that IRS did not acknowledge receipt of tax data received by mail from the records centers. (See pp. 68 and 69.)

IRS is aware of many of these problems. Its Internal Audit Division has performed many security-related reviews and issued numerous reports to management identifying security problems. Although this has resulted in security improvements, many weaknesses remain.

GAO's 32 recommendations designed to correct specific weaknesses are included at the ends of chapters 3 through 8 and cover the following specific areas:

--Computer operations. (See p. 18.)

--The data retrieval system. (See p. 34.)

--Employee access to printed data. (See p. 44.)

--Background investigations. (See p. 53.)

--Physical security. (See p. 65.)

--Tax data at Federal Records Centers. (See p. 70.)

IRS agreed with the majority of these recommendations. The Commissioner of Internal Revenue said that, although IRS has not been as aggressive in the past as it might have been in correcting situations that potentially weakened its overall security posture, he is committing the Service to a vigorous course of improvement. The relatively few actual losses or disclosures probably contributed, he noted, to a feeling among IRS management that security of tax data was not a major problem. Now this feeli[illegible] is being changed. To this end, [illegible] said, IRS has started to improve its [illegible]itude about the need for maximum secu[illegible] of tax information and to be sure of obtaining compliance with existing security requirements by:

--Devoting a considerable portion of a recent conference of regional commissioners and district and service center directors to a discussion of means of obtaining compliance with security requirements and procedures.

--Starting a security awareness program for all employees.

--Beginning to use its existing evaluation programs more effectively to monitor compliance with security requirements.

--Undertaking a major "risk analysis" effort to identify and rank the threats to operations and the confidentiality of tax information.

--Approving in concept the creation, testing, and evaluation of full-time district office security officer positions in one region.

--Starting to develop major training to instill sound security principles in all Service supervisors and managers.

IRS agreed to carry out GAO's recommendations to correct specific weaknesses in the areas of the data retrieval system, employee access to printed data, background investigations, physical security, and tax data shipment. While agreeing to most of GAO's recommendations on computer operations, IRS stated that other actions being taken might preclude the need to implement certain recommended controls over program documentation and tape library access. IRS, therefore, intended to study these recommendations further. The Commissioner disagreed with the need for records identifying, at one computer facility where most work involves testing, the magnetic tapes used and who accessed them. (See p. 21.)

GAO believes that effective implementation of its recommendations should result in a sound IRS security program to protect tax data confidentiality.

Contents

CHAPTER Page

APPENDIX

ABBREVIATIONS

GAO	General Accounting Office
IRS	Internal Revenue Service

CHAPTEk 1

INTRODUCTION

> "During the last few years the daily newspapers have been filled with accounts of racketeers, blackmailers, and kidnapers. In my opinion the publication of these lists (taxpayers names and assessments) will be one of the greatest incentives to crime that can possibly be imagined. The Dillingers, the Carpis, and the 'Baby Face' Nelsons and their ilk will eagerly scan each list in his own community for a clue as to possible profitable victims. So far as this criminal element is concerned, the Government, in effect, will be furnishing a 'who's who' list of prospects. It might just as well furnish these lists to the kidnaper and racketeer direct and be done with it."

Although this statement appeared in the Congressional Record more than 40 years ago, 1/ the need for confidentiality of tax information continues to be a strongly held and often expressed public concern.

In response to this concern, the Congress has historically attempted to restrict the disclosure of tax return information, even to the point of limiting its own inspection privileges. Its most recent effort--The Tax Reform Act of 1976--was signed into law on October 4, 1976. This act strengthened the existing law regarding disclosure of tax return information and increased the penalties for unauthorized disclosure. It also increased the Internal Revenue Service's (IRS) responsibility for protecting tax return confidentiality.

IRS recognizes the need for confidentiality of tax return information. In 1973 the IRS Commissioner testified before a Subcommittee of the House Committee on Government Operations:

> "In my judgment, preserving the confidentiality of income tax returns and tax information is of primary importance in maintaining taxpayer compliance and public confidence in our tax system * * * To the extent that sound reasons do not require the

1/Testimony of Representative Robert L. Bacon given on Feb. 27, 1935, before the House Committee on Ways and Means (120 Congressional Record 2690).

> Service to open up tax returns to others, the Service should guard the taxpayer's right of privacy."

At the same hearings, IRS' Chief of the Disclosure Staff stated:

> "The right to personal privacy is manifest in the provisions of the Constitution and the Internal Revenue Code. We believe that voluntary compliance with the Federal tax laws is enhanced by the statutory provisions for the confidential treatment of income tax returns. The indiscriminate disclosure of any tax information would be regarded as an unwarranted invasion of the taxpayer's right to privacy concerning information furnished to IRS for tax administration purposes. A heavy burden is placed on the Government to maintain a proper equilibrium between the acquisition of information and the necessity to safeguard privacy."

While both the Congress and IRS recognize the need for confidentiality, they have also recognized that, on occasion, third parties need access to tax return information. The current tax law restricts disclosures of tax information to specific third parties. Section 6103 of the Internal Revenue Code includes specific provisions regarding who can obtain access, under what circumstances, and how the recipient must safeguard information obtained. Legally designated recipients include certain congressional committees, the President, Federal agencies, State taxing authorities, taxpayer designees, and persons having a material interest.

To reinforce the need for confidentiality, the law provides penalties for unauthorized disclosure. Convicted Federal employees must be dismissed from office or discharged from employment. For Federal and State employees, the law's felony provisions set a maximum penalty of a $5,000 fine, 5 years in prison and prosecution costs. Similar felony penalties apply to:

--Any person who prints or publishes tax data obtained through an unauthorized disclosure.

--Any person who offers an item of material value for any return or return information.

--Any corporate shareholder who legally receives corporate tax data and subsequently makes an unauthorized disclosure of it.

ORGANIZATION AND WORKLOAD: THEIR EFFECT ON SECURITY

IRS' size, its organization, and the volume of tax data it handles make security a formidable task. As size and volume increase, so does the possibility for unauthorized disclosure.

Headquartered in Washington, D.C., IRS has a national computer center, a data center, 7 regional offices, 10 service centers, 58 district offices, and about 900 local (posts of duty) offices. Nationally, it employs about 86,000 people. As would be expected, tax data can be found throughout the organization.

Within the organizational framework:

--The national office develops broad nationwide policies and programs for administration of tr internal revenue laws and related statutes, and directs, guides, coordinates, and controls IRS' endeavors.

--The national computer center maintains and updates taxpayer account master files and produces from them magnetic tapes, microfilm, records, and tax data for use by IRS and others.

--The data center performs nonmaster file data processing operations, including preparation of various IRS fiscal, statistical, and management reports. Some of the reports incorporate tax data extracted from tax returns and other taxpayer identifiable records. The center also processes the Department of the Treasury payroll.

--The regional offices execute broad nationwide policies and programs to administer the internal revenue laws, to carry out appellate programs, and to direct and coordinate the functions and activities of the district offices within the region.

--The district offices administer the internal revenue laws in conformance with Service policies and programs established by the national and regional offices.

--The service centers process tax returns and related documents through the use of automatic and manual data processing systems and high-speed processing devices, perform some audit functions, and maintain accountability records for internal revenue taxes collected.

Annually, the 10 service centers receive and process about 125 million tax returns. Processing generates millions of other documents containing taxpayer identifiable data, such as computer generated taxpayer transcripts, microfilm transcripts, management information reports, investigation reports, and correspondence.

Once processed, IRS stores tax returns at Federal Records Centers--individual income tax returns for a minimum of 6 years and corporate returns indefinitely. The General Services Administration operates the records centers.

SCOPE OF REVIEW

The Joint Committee on Taxation requested that we review the adequacy of IRS' internal and external controls to assure that access is limited to only IRS employees and others authorized by law who have a need to examine tax returns and to assure that adequate records are maintained to identify all persons who access a specific tax return or taxpayer identifiable data. Taxpayer identifiable data includes almost all information IRS receives or prepares, in addition to the tax return itself. We focused primarily on internal controls and did not review third party security over tax data disclosed to them by either the taxpayer or IRS.

IRS has proposed the acquisition of a computerized tax administration system. In a previous report,[1] we evaluated the ability of the proposed system concept to adequately protect taxpayer information. We stated that the capability of the system to do this could not be conclusively evaluated before system design and implementation. However, with proper design and implementation, the system could provide a high level of protection. In making our assessment, we addressed certain weaknesses in the existing system and automatic data processing environment that could, and should, be corrected in the design and implementation of the proposed system. We also stated that our assessment of the existing system would continue.

This report pertains only to IRS' existing system for safeguarding taxpayer data. It addresses some of the same

[1] "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System," LCD-76-115, Jan. 17, 1977.

matters covered in the previous report, but in more detail. It also addresses broader security issues not pertinent to the previous report.

We examined IRS policies, procedures, and practices for providing security over access to tax data and

--interviewed agency officials,

--observed the physical facilities at selected IRS locations,

--reviewed and analyzed IRS computer operations and controls, and

--reviewed agency files.

We also reviewed physical security and security practices at two Federal Records Centers.

We did our work at IRS' national office;. National Computer Center, Martinsburg, West Virginia; Detroit data center, Chicago and Dallas regional offices; Salt Lake City, Detroit, Des Moines, and Dallas district offices; Kansas City, Missouri, and Ogden, Utah, service centers; various local posts of duty; and Federal Records Centers at Denver and Kansas City.

Security reviews at these and other IRS locations have been made by various internal IRS groups. Numerous IRS Internal Audit reports on security problems were issued to management prior to, during, and subsequent to our review. And, IRS management said they would take corrective action in many cases. Some of our tests, both in format and results, closely parallel some of those applied by Internal Audit, especially in the areas of computer operations and the data retrieval system. While Internal Audit's efforts have resulted in security improvements, our recommendations focus on remaining weaknesses.

CHAPTER 2

IRS' SECURITY PROGRAM DOES NOT ADEQUATELY

PROTECT TAX DATA CONFIDENTIALITY

IRS' security program, while generally sound in concept, does not adequately protect tax data confidentiality. Widespread opportunities for unauthorized disclosure existed throughout IRS because it did not adequately implement or design security procedures and controls. An untrustworthy IRS employee and others could penetrate the system, obtain unauthorized tax data and not be detected.

IRS faces several problems in protecting tax data confidentiality. Internally, IRS has volumes of taxpayer data in several formats. Many of IRS' 86,000 employees need access to some of this data, and excessively tight controls over such accesses could impede efficient tax administration. And perfect security within IRS, even if attainable, would not guarantee the confidentiality of a vast volume of tax data outside IRS' control.

To secure tax data under its control, IRS, in most instances, designed procedures and controls to limit access to those employees and others that need the data. In practice, however, IRS relies heavily on the integrity of its employees and others rather than strict enforcement of its regulations. As a result, these persons have relatively free access to large volumes of tax data.

Because widespread opportunities exist for access to tax returns and tax data, IRS has difficulty identifying persons responsible for unauthorized disclosures. During fiscal year 1976, IRS' Internal Security Division investigated 182 allegations of such disclosures and identified responsibility for 43. Of the 43 persons identified as disclosing tax data, 37 received disciplinary actions, including suspension, reprimand, or demotion, and 6 were separated from employment. Data was not readily available from IRS concerning whether disclosures had actually occurred in the remaining 139 cases and, if so, the reasons why responsibility was not identified.

THE THREATS TO CONFIDENTIALITY

IRS must safeguard against threats to the confidentiality of tax returns and tax data under its control. Yet, many organizations and persons outside IRS have copies of returns and tax data. Taxpayers retain copies of their returns, some States require taxpayers to submit a copy of the Federal return with the State return, and tax preparers retain copies of client returns (about half of all taxpayers in 1972 used the services of a professional or commercial practitioner). Obviously, IRS cannot control the confidentiality afforded this tax data.

But what about tax data within IRS' control? Untrustworthy employees, non-IRS employees granted access to IRS facilities, and outside penetrators constitute the major threats to its confidentiality.

The dishonest or untrustworthy employee poses the greatest threat. The employee has immediate access to the facility and can more easily obtain the knowledge necessary to retrieve and, if necessary, interpret the desired data. The employee also has the greatest chance of requesting and obtaining tax data through normal channels.

Non-IRS personnel granted access to the facilities and to areas within the facilities where sensitive data is located pose the second greatest threat

The outside penetrator poses the lesser of the three threats. To successfully penetrate the system and obtain the desired tax data, the outside penetrator must first gain knowledge of security measures in effect, especially their limitations. Also, the penetrator must learn the data's location, how to retrieve it, and, if necessary, how to interpret it.

These threats can be minimized through vigorous application of well-designed security safeguards. These safeguards must include controls to prevent outsiders from gaining access and to prevent IRS employees and others from accessing tax data not needed to perform their duties.

IRS' SECURITY PROGRAM: AN OVERVIEW

IRS' security program includes various safeguards designed to protect the confidentiality of tax data against both the untrustworthy employee and others. The program and the responsibility for its implementation is complex and delegated throughout the organization.

The program

IRS designed its security program to provide reasonable, as opposed to total, protection. IRS, under this concept, considers a building's structure, use, and location; whether the public needs access; and the type of equipment, complexity of operations, and concentration of tax data.

IRS defines normal protection as that provided by a building locked or guarded after hours, a locked room in a building open after hours, a key-locked file cabinet in a facility open to the public, or the presence of a Government employee. Normal protection is the security level commonly afforded any document that does not contain tax data.

IRS has properly decided that tax returns and tax data need more than normal protection and it established a numerical system of points to identify the level of physical protection required for every form of tax data. It also assigned protection points to various security features. IRS attempts to use those security features that will give the tax data the protection required.

The security program design includes not only physical features but internal controls. Physical features utilized by IRS include locked rooms, locked and guarded buildings, electronic security systems, fences, and identification systems. IRS supplements physical features by employing internal controls over computer operations, designating certain areas as restricted access, specifying disposal methods for tax returns and related information, and conducting employee background investigations.

Program responsibilities

Recognizing the need for an overall perspective, IRS established a Security Council in 1973 to provide direction for IRS' security efforts. The Council, chaired by the Assistant Commissioner for Administration, includes six other Assistant Commissioners as members, each being responsible for a different facet of IRS operations. Council responsibilities include formulating and presenting security policy recommendations to the Deputy Commissioner and Commissioner for final decision.

However, IRS did not assign total responsibility for developing procedures and controls to implement security policy or for evaluating day-to-day compliance with prescribed procedures to any one office or organization.

Rather, Assistant Commissioners share these responsibilities as follows:

Security area	Responsible Assistant Commissioner
Access to plant and documents	Administration
Authorized disclosure	Compliance
Computer operations	Accounts, Collection, and Taxpayer Service
Investigation of unauthorized disclosures and employee background investigation activity	Inspection

Through delegations and redelegations, responsibility for the day-to-day implementation of security guidelines has passed down through IRS' organization to designated individuals in each field installation. Each organizational level, however, retains some responsibility for planning, developing, evaluating, and managing the security program for its own area.

Field personnel can have duties beyond security. Besides being responsible to an Assistant Commissioner for a facet of security, they can also be responsible to the director of the field installation for other duties. For example, the data retrieval system security administrator in a district office is also responsible to the district director for part of the district's collection program. Accordingly, the security program implemented depends on the attitudes of local management and the priorities each incumbent establishes for security.

IRS' Internal Audit Division, as a part of its overall responsibility, identifies security problems through its reviews. As a result of these efforts, numerous reports have been issued to management on such subjects as the data retrieval system, computer operations, physical security, and mailing and disposing of tax data. Internal Audit plans to continue this effort and has programmed 1,105 staff days for calendar year 1977.

OUR OVERALL IMPRESSION

Implementation weaknesses and certain program shortcomings have resulted in a potential for widespread unauthorized disclosures. Because of these weaknesses and shortcomings, security safeguards could easily be penetrated--especially by IRS employees and others having access to the facilities.

Depending on the position occupied, an employee could obtain, without detection, tax returns or tax data on preselected taxpayers. Employees and others having access to the facilities could obtain tax data on a large number of taxpayers at random.

The specific weaknesses leading to our conclusion are discussed in subsequent chapters. Some of the more significant weaknesses include

--conditions in computer operations that could result in relatively easy unauthorized access to large quantities of taxpayer identifiable data;

--supervisors failing to adequately monitor tax data requests, thereby making it possible for employees to obtain unneeded tax data;

--shortcomings in implementing controls over shipped tax data, microfilm tape inventories, and after hours security, thereby greatly increasing the chances for unauthorized disclosures;

--shortcomings in security program requirements for employee background investigations resulting in placing employees in sensitive positions without adequate screening for trustworthiness; and

--non-IRS employees being permitted access to areas containing unsecured tax data.

These problems exist largely because no one organizational unit in IRS is responsible for security. Consequently, IRS did not uniformly implement security guidelines nor place enough emphasis on complying with prescribed procedures. Setting up the Security Council represented a step forward but did not centralize security responsibilities.

In a January 1977 report, we assessed the capability of IRS' proposed Tax Administration System to safeguard taxpayer information. [1] We recommended that IRS establish a national data processing security office and a similar office at each data processing facility responsible for administrative, physical, and technical security. As a

[1] "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System," LCD-76-115, Jan. 17, 1977.

result, IRS is currently studying the merits of a national security office concept. IRS officials said they plan to expand the study to include all facets of security rather than just data processing.

We question IRS' need to study the merits of a national office concept. It is clear from our work that such an office is needed. Responsibility for tax data security must be clearly defined, and a continuing program established to insure that tax data is properly safeguarded. Therefore, focusing a study on exactly how to set up a central office would be more appropriate.

RECOMMENDATION TO THE COMMISSIONER OF INTERNAL REVENUE

We recommend that the Commissioner of Internal Revenue establish an independent office responsible for all facets of the security program at all IRS facilities. This office should be directly responsible to the Commissioner for developing procedures and controls to implement IRS' security policy. It should also be responsible for monitoring compliance at all IRS facilities and reporting all instances of noncompliance to local management and the Commissioner.

IRS COMMENTS

In a May 31, 1977, letter, the Commissioner of Internal Revenue agreed with this recommendation and said that IRS is presently determining the proper organizational location and plan for implementing such an office. (See app. I.)

The Commissioner noted that IRS' long organizational history with a low experience of actual losses or disclosures has contributed to a feeling among management officials that security of tax data has not been a major problem. He said that although IRS has not been as aggressive in the past as it might have been in correcting situations that potentially weakened the overall security posture, he is committing the Service to a vigorous course of improvement. To this end, he said that he has started efforts to improve IRS attitudes about the need for maximum security of tax information and to insure compliance with existing security requirements.

CHAPTER 3

NEED TO IMPROVE CONTROLS

OVER COMPUTER OPERATIONS

IRS uses computers to process, store, and retrieve vast amounts of tax data. Confidentiality of this data cannot be adequately assured because IRS controls over its computer operations are lax. IRS employees and others have many opportunities to obtain data without detection. For example:

--Programmers could easily run an unauthorized program or make an unauthorized program change.

--Employees and others could obtain unauthorized access to magnetic tapes containing tax data.

--Unauthorized persons could obtain printed products containing tax data.

NEED TO STRENGTHEN CONTROLS OVER PROGRAMMERS AND ANALYSTS

IRS programmers and analysts--computer specialists--write, test, and analyze national office, National Computer Center, Detroit data center, and service center computer programs. They know about the operations of computers and tape libraries. Therefore, they have the ability and knowledge to manipulate computer operations.

They also have the opportunity. A number of weaknesses exist in IRS' controls over programmers and analysts. For example:

--Regulations do not require periodic reviews to ascertain whether programmers write only authorized programs or whether the programs being run contain unauthorized modifications.

--Because checkout procedures have not been established, programmers and analysts can freely access program documentation explaining what a program accomplishes and how.

--Programmers and analysts can remove tapes containing tax data from the tape library without a chargeout and also can operate the computer at some IRS data processing facilities.

--Programmers and analysts use actual tax data to test their programs and program modifications rather than using test data. At Kansas City, a service center official said they use actual tax data without having to obtain special authorization. At Ogden, service center officials said they obtain telephone approval from the IRS national office, but no record of these approvals exists.

Having access to program documentation and tape files, and possessing both the ability and opportunity to operate the computer, programmers and analysts can make unauthorized programs or program changes and use the computer for unauthorized purposes. They could easily become unauthorized creators and disseminators of tax data.

NEED TO LIMIT ACCESS TO COMPUTERS

IRS regulations do not specify who may or may not operate the computers. Ideally, controls should limit access to personnel specifically designated as computer operators. Necessarily, however, IRS must allow computer manufacturer personnel to service the computers. But other personnel, such as programmers, analysts, and schedulers have operated the computers. Moreover, IRS has allowed the manufacturer personnel to operate the computers unobserved.

Computer manufacturer engineers must be allowed access to the computers to solve electronic and mechnical problems. Whenever they perform maintenance work, IRS guidelines require that computer operators or other computer personnel be present. However, at Ogden, the engineers worked on the computers on a holiday when no Ogden employees were present; and, at the national office computer facility--a satellite office of the National Computer Center--an engineer works alone from midnight to 8:00 a.m. Not only could the engineers make unauthorized use of the computer, they also had unrestricted access to an adjacent tape library. Under these conditions an engineer could easily run an unauthorized program.

Unauthorized programs could be run with little chance of detection under existing controls. IRS attempts to identify the programs that have been run through machine utilization reports, some manually prepared and others computer generated. Manually prepared reports do not provide a good control because of the assumption that a person running an unauthorized program will record it. Computer generated utilization reports show the programs that were run but do not identify the operator.

Access to computers

Unauthorized access to IRS computers can and has occurred. Weaknesses in national office computer facility procedures demonstrate the potential for unauthorized access. An event at Ogden shows that it has happened.

At the national office computer facility, supervisors do not approve programs and job requests submitted by programmers. Although the job request lists the serial numbers and file identifications of the magnetic tapes which will be accessed, the programmer's name and programmer number, and any special instructions to the computer operator, no controls exist to show whether a programmer used the correct programmer number and name. Further, the national office computer facility does not record who used what tape and for what purpose. Because of these weaknesses, any individual familiar with the facility's operating practices could gain access to tax data with little chance of detection.

At the Ogden service center, procedures and controls did not detect an unauthorized access to the computer. An employee who had formerly been a national office computer programmer performed some occasional programming for the service center, although not assigned to the computer branch. On three successive days, he had unauthorized programs pertaining to a course he was taking at a local college run on the Ogden computer by giving a deck of computer cards, his programmer number, and a project run number to the computer scheduler. The scheduler said he knew this employee was authorized to submit programs; however, he did not notice that the employee was submitting an unauthorized program. The computer scheduler learned about the unauthorized run when another student, lacking a programmer number, also submitted his class project. Although evidence indicates that no taxpayer identifiable data was obtained, it could have been.

NEED FOR BETTER CONTROL OVER MAGNETIC TAPES

IRS computer personnel did not adequately control access to magnetic tapes containing tax data and could not account for some tapes. One reel of magnetic tape can contain information on about 5,000 taxpayers. If a tape falls into the hands of an unauthorized person who has access to a computer, much tax data could be disclosed.

Tape library controls

Tape libraries are freely accessible by other than tape library personnel. IRS guidelines specify that a tape library should be a restricted area with access limited to specified personnel. However, IRS officials have extended access privileges to about everyone that is permitted into the computer room. Such extensive access tends to defeat the purpose of a restricted area and leads to a lack of control over tapes.

At the Kansas City and Ogden service centers, and the national office computer facility, tape libraries are located in or adjacent to the computer rooms. Once into the computer rooms, one may walk into the tape libraries through unlocked doors. At Kansas City and Ogden, the director and his assistant, the division chief over computer operations and his assistant, as well as computer branch employees are allowed into the tape library. At Kansas City, the librarian cannot observe traffic into or out of the library. At Ogden, an official said the tape library should be restricted to tape librarians; however, programmers were allowed to get their own tapes. At the national office computer facility, IRS analysts and the computer manufacturer engineers had offices on the opposite side of the library from the entrance of one computer room, resulting in constant foot traffic through the tape library.

Tape chargeout records can provide accountability over tapes leaving the library. Recognizing this, IRS guidelines provide that no tapes leave the library without being charged out. However, the installations visited frequently did not follow established procedures.

--At Ogden we observed computer programmers removing tapes from the library without charging them out.

--On one selected day at Kansas City, we found 65 tapes located outside the tape library without being charged out.

--At the Detroit data center, a check of 10 tapes containing sensitive data and located in the computer room showed that 9 were not properly charged out of the tape library.

--At the National Computer Center, tape librarians were not maintaining copies of chargeout forms or maintaining any record to show what tapes had been removed from the library.

--At the national office computer facility, which has two tape libraries, tapes taken to the computer room for processing are not charged out at either library.

--And, at one of these libraries, tapes are not charged out even when they are to be removed from the immediate area of the computer facility.

Unless librarians follow prescribed procedures, they cannot account for tapes removed from the library.

Inventory controls

IRS procedures require an annual magnetic tape inventory. Inventory results showed that magnetic tape controls were ineffective. For example, a January 1976 inventory at Ogden showed 44 tapes missing; by April 1976, Ogden found them all. An April 1976 inventory at Kansas City showed 738 tapes missing; by May 21, 1976, 80 tapes still could not be accounted for. The National Computer Center found 33 tapes missing when taking its May 1975 inventory. The Detroit data center took a partial inventory in 1975 but did not retain the inventory records. A national office computer facility official said although exempt from the requirement they took semiannual inventories. He said, however, no records of the inventories were retained but he recalled that about 16 tapes were missing at the last inventory.

The IRS inventory results prompted our taking test inventories. Results showed that:

--Ogden did not count computer disks which also serve to store tax data. We took an inventory and found two disks missing. These two disks were still missing when we left the center 13 weeks later.

--In 1975 the Detroit data center counted only part of its tapes. Also, the record which lists all tapes at the center contained inaccuracies because IRS did not adjust for tapes disposed of and did not include test data tapes. Of 301 tapes we tried to account for, 27 could not be located.

--The national office computer facility tape location listing was inaccurate for 8 of 50 randomly selected tapes. IRS employees found four of the eight tapes.

--National Computer Center records did not identify tape locations. This necessitates a complete search of the center to find a tape. We previously identified and reported on this problem during our review of the proposed Tax Administration System. [1]

Without following its procedures for limiting access to tape storage areas and for preparing tape chargeout records, IRS cannot protect the confidentiality of tax data stored on magnetic tapes. Failing to follow these requirements, IRS cannot account for many tapes or be sure of the exact number missing. Taking proper inventories of tapes and disks would permit IRS to determine the number missing and evaluate the effectiveness of other controls.

PRINTED PRODUCTS NOT CONTROLLED TO ASSURE RECEIPT BY AN AUTHORIZED REQUESTER

Computer-printed products can contain information on hundreds of taxpayers. Like any other tax data, printed products should be controlled to make certain that only authorized personnel obtain access. IRS controls in this respect were almost nonexistent.

Neither the Kansas City center nor the national office computer facility required the authorized recipients to sign for printed products. At Ogden, the recipients signed for some printed products by initialing a routing form; however, a service center unit distributes the more voluminous products without obtaining receipts. Kansas City uses a checkoff list to indicate those products which have been picked up.

At the national office computer facility, card decks, job requests, and any resulting products are left on shelves in a nonrestricted area of the facility. Users pick up the products but do not sign for them. The facility makes an exception for certain intelligence and audit jobs by keeping those printed products in a filing cabinet until picked up. The user must, however, request this procedure and even then does not sign for the documents.

Under these systems of distribution, IRS would not know whether an unauthorized person picked up a printed product

[1] "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System," LCD-76-115, Jan. 17, 1977.

unless the authorized user complained about not receiving the data. Reliance on a complaint system is inadequate.

CONCLUSIONS

Programmers and analysts possess the capabilities and have the opportunity for unauthorized and undetected manipulation of the data processing system. Present procedures provide programmers and analysts the opportunity to write unauthorized programs and run them on the computer without being readily detected. To prevent unauthorized disclosures and unauthorized computer use, programmers and analysts must be placed under adequate controls.

Programmers and analysts are not the only ones who pose a threat of unauthorized disclosures. Other IRS personnel and computer manufacturer engineers who have access to the computer area also pose a threat because of procedural deficiencies regarding computer room operations. Procedures must be implemented to stringently control magnetic tapes, restrict access to the computer, and assure that only authorized persons receive computer-printed products.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

To improve controls over computer operations, we recommend that the Commissioner of Internal Revenue:

--Establish a procedure whereby programmers and analysts must obtain written authorization from the national office before using actual tax data for testing.

--Establish a procedure for periodic review to determine that programs and program modifications are authorized.

--Establish a checkout procedure for program documentation.

--Establish guidelines to govern who may and may not operate the computers.

--Require that computer personnel closely monitor equipment manufacturer engineer activity.

--Establish procedures whereby national office computer facility job requests receive supervisory approval and tape librarians maintain records identifyinq the magnetic tapes used and who accessed them.

--Require that tape library access be restricted to library personnel and that tape chargeout records be properly prepared and maintained.

--Revise inventory guidelines to require that all magnetic tapes and disks be periodically inventoried at all tape libraries, that inventory results be reconciled to the tape records, and that missing tapes and disks be accounted for.

--Establish a uniform procedure whereby authorized requesters sign for receipt of computer-printed data.

IRS COMMENTS

IRS agreed with most of our recommendations to improve security over computer operations and cited actions which it has taken or plans to take to remedy the reported weaknesses. (See app. I, pp. 73 to 76.) For example, IRS said that it:

--Will establish procedures for limiting the use of actual tax data for testing purposes and for requiring the approval of designated personnel when used.

--Is developing automated program modifications, an authorization and control system with audit trails of updates, procedures for periodic matching of field software with national office masters, and will assign responsibility for assuring that only authorized production programs are run and that program modifications are authorized.

--Will establish and immediately issue guidelines governing who may and may not operate the computers.

--Will reemphasize the need to closely monitor equipment engineer activity and will check periodically the extent of monitoring being performed.

--Will revise guidelines to require supervisory approval of national office computer facility job requests.

--Will establish a requirement for semiannual magnetic tape and disk inventories.

--Will issue procedures to provide for maintaining a standard log indicating the disposition of printed data and punched cards, and for a receipt procedure system.

IRS agreed with the need to control program documentation but believed that actions being taken in response to other recommendations may preclude the need for checkout procedures. It pointed out that it will establish controls requiring that only computer operators be allowed to operate the computer and will exercise stricter controls over programs and program modifications. IRS said that, in view of these actions, it will review its controls to determine whether checkout procedures should be established for program documentation.

The other actions IRS agreed to take will certainly strengthen security over computer operations. However, a function of internal control is to provide assurance that errors and irregularities may be discovered with reasonable promptness, thus assuring the reliability and integrity of computer operations. For security purposes, the controls established should provide a trail to identify unauthorized access to program documentation and the persons making an unauthorized program modification. Program documentation checkout procedures are one means of providing such a trail. In reviewing the need for establishing such checkout procedures IRS should bear in mind that unless these objectives can be met through other means, checkout procedures should be established.

IRS also agreed that tape chargeout records should be properly prepared and maintained and that tape library access should be restricted but felt that there are occasions when other than library personnel need access. As an example, on weekends when library personnel are not on duty, operating personnel may need library access due to unforeseen problems, reruns, errors, etc. IRS also pointed out that current procedures restrict library access to library personnel, computer branch chiefs, data retrieval system security administrators, and those persons specifically approved by the computer branch chief. Current procedures also make library personnel responsible for documenting the removal of all tapes and disks from the library.

We recognize that there may be occasions when other than library personnel need access to the tape library but believe that established internal controls should encompass such instances. Good security dictates that established controls provide a record of all library accesses as well as the tapes and disks that were removed and returned. Any exception will compromise security. While there are several ways to control accesses in the absence of library personnel, one approach could be to require documentation of the need for such access, specific approval by the computer branch chief on a case-by-case basis, witnessing of the access by an appropriate supervisor, and making appropriate entries to the chargeout records. Whatever the techniques used, control and accountability must be present at all times or security is lost.

IRS disagreed with our recommendation that national office computer facility tape librarians maintain records identifying the magnetic tapes used and who accessed them. It said that approximately 1,000 computer tests are run by the facility on a daily basis, each using several reels of tape and that maintaining the recommended records would be prohibitively expensive and cumbersome. Considering that the facility is used primarily for testing, IRS felt that the degree of risk involved would not justify the expense.

We agree that the bulk of the facility's work is of a testing nature. But, actual tax data is sometimes used in the testing. The facility also supplements the production operations of the National Computer Center by making production runs using tapes containing actual tax data. The presence of actual tax data in the tape library and the sheer volume of tape activity dictates some form of control to identify which tapes have been used and who used them.

Notwithstanding the need for security and accountability controls over actual tax data, test tapes themselves often represent substantial investments of time, research effort, and knowledge. They are assets to be protected and the first ste, in this regard is being able to account for them at any given time.

Tape library controls are generally considered a fundamental part of the internal control system for computer operations. Records of the tapes used and who used them can provide tape accountability, enhance the physical protection of tapes, and provide a trail to detect unauthorized use.

In lieu of such records, IRS should assure that its system of internal controls over national office computer facility operations provides adequate tape accountability and trails for detecting unauthorized use.

CHAPTER 4

THE DATA RETRIEVAL

SYSTEM CAN BE PENETRATED

The data retrieval system--one of IRS' computer systems--contains computerized records on about 10 percent of all taxpayers. IRS selects taxpayer records to be placed on this system based on the probability of need to quickly obtain data for responding to taxpayers' inquiries about their account status or for accomplishing certain day-to-day operations.

The system can be accessed through about 4,000 visual display terminals. Through these terminals, about 18,600 authorized service center, district office, and local office employees can

--instantaneously access a taxpayer's account,

--view the recorded data on a visual display screen and generate a printout,

--change the recorded data,

--cause taxpayer notices of various kinds to be mailed,

--request original tax returns or photocopies, and

--have records for almost any taxpayer placed on the system.

The system design includes safeguards to deny unauthorized access and to limit authorized users in terms of transaction types and terminal locations. IRS recently made procedural changes to strengthen data retrieval system security. But weaknesses remain which could result in unauthorized access to and disclosure of taxpayer data.

RETRIEVAL SYSTEM SECURITY FEATURES

System security is based primarily on internal control features built into the computer. These features control access to the system and limit user privileges. To supplement these internal features, a designated security administrator at each service center and district office monitors system security. Security supervisors assist each security administrator by overseeing system users during work shifts.

System users make initial system access by activating the computer terminal with an individually assigned secret password and other identification data. Special computer programs generate the secret passwords and produce a list of alternates to be used in the event one is lost or compromised. Guidelines require periodic changing of passwords and the security administrator furnishes the new ones in sealed envelopes to authorized users. Unless the password and identification data input by the user match information in the computer, initial access is denied.

The system controls the extent of user access through employee and terminal profiles containing identification data and system command codes. Profiles limit what transactions can be performed by an authorized user and on which terminal. Each employee and each terminal has a profile. The data and command codes in the employee and terminal profile must agree before the system will accept a transaction.

A command code tells the system what to do. The system contains three types of command codes--security, production, and training. System security personnel use security command codes for such purposes as establishing, modifying, and deleting employee and terminal profiles. System users use production command codes to access and adjust tax data in the system. Training command codes, obviously, are used for training. Each code instructs the computer to perform a specific operation in relation to the transaction entered and the data recorded in the system. The number and combination of command codes granted to a user determines the user's capability to process or obtain data.

Other security features of the data retrieval system include a

--control which locks a terminal after three consecutive errors;

--capability to designate a taxpayer account as restricted, thereby limiting the number of system users permitted access to it;

--capability to detect system users who access their own tax records;

--computer generated daily security report of the violations detected by the system; and a

--tape record showing transactions processed and accounts accessed by each user.

THE DATA RETRIEVAL SYSTEM DID NOT REPORT CERTAIN SECURITY VIOLATIONS

We tested the adequacy of retrieval system security features by first assuming the role of an unauthorized user and then a security supervisor. Initial testing was at the Kansas City service center during July 1975 with subsequent testing at both the Kansas City and Ogden service centers during February 1976.

The unauthorized user tests were to determine if security features could be circumvented to gain system access. Results showed that to access the data retrieval system the user needed a valid password, name, and social security number. We attempted invalid entries and the system denied access. After the third invalid entry, the terminal locked--a system security feature activated by three consecutive errors. We concluded that these security features adequately protected against circumvention by an unauthorized user.

We then tested security in the role of a security supervisor. Security supervisors can process transactions as well as change both employee and terminal profiles. They are also issued a security manual which describes the system security features. Considering these factors, the security supervisor represents the lowest level within IRS having the capability of circumventing many of the system's internal security features.

After receiving a password and having appropriate profiles established for our use, we tried to use command codes that were not in our employee and terminal profiles. The system properly denied us access and the security violations flashed on the terminal screen. Next, we unsuccessfully attempted to access a dummy restricted account and the system properly recorded the attempt on the daily security report. IRS has since implemented other systemwide controls over restricted accounts by (1) causing an account restricted by one service center to be restricted servicewide and (2) limiting the number of terminals capable of accessing restricted accounts.

The security manual states that changing one's own profiles is prohibited. During our July 1975 testing, however, we successfully changed both our employee and terminal profiles by using the security command codes that security supervisor profiles contain. Neither change appeared on the daily security report to alert the security administrator.

IRS officials, after reviewing our test results, modified the system so that the daily security report included such transactions. Our February 1976 testing confirmed this change. Since then, IRS has further modified the system to automatically deny users access while their profiles are being updated, and to show all employee and terminal profile changes on the daily security report. These modifications should improve system security.

The security manual states that accessing or changing one's own tax account is a security violation which will be reported on the daily security report. However, in our July 1975 testing we succeeded in issuing ourselves a refund by using a combination of command codes. The transaction did not appear on the daily security report.

Again, IRS corrected the problem. The first step in issuing ourselves a refund during the July 1975 testing was to change our employee number. In the February 1976 testing, the system properly denied this attempt and reported it on the daily security report. Subsequent to our February 1976 testing, IRS further modified the system to report all employee number changes on the daily security report. This should improve security since it will allow the security administrator to detect questionable or unauthorized changes.

Besides these tests, we evaluated retrieval system security in our prior review of IRS' proposed tax administration system. [1] The previous review identified certain weaknesses and the report contained related recommendations. As a result of these recommendations and its own initiative, [2] IRS improved system security, but other weaknesses remain. These weaknesses and recommended solutions are discussed below.

UNAUTHORIZED COMMAND CODES IN EMPLOYEE AND TERMINAL PROFILES INCREASE CHANCES OF UNAUTHORIZED ACCESS

A major aspect of security in a data retrieval system is limiting user privileges. Recognizing this, IRS regulations state that user profiles should contain only those

[1] "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System," LCD-76-115, Jan. 17, 1977.

[2] IRS' Internal Audit Division had also reported on similar type problems.

co.:mand codes required t.o perfoım the.ir specific dut.ies and that the national office must approve anv deviations. Contrary to this requirement, numerous employee and terminal profiles contained command codes in excess of those authorized by IRS guidelines. This condition provided users the opportunity to make unauthorized access to tax data and unauthorized adjustments to tax accounts.

The security manual provides that only certain command codes, determined by function, be issued to certain terminals and users. We selected terminal and employee profiles being used and compared them with the profiles authorized by the manual. As shown in the following table, more than 60 percent of the employee profiles and 84 percent of the terminal profiles contained unauthorized codes.

	Number of terminal profiles			Number of employee profiles		
	Reviewed	Having un-authorized codes	Percent in error	Reviewed	Having un-authorized codes	Percent in error
Kansas City service center	10	8	80	21	a/17	81
Ogden service center	7	7	100	10	10	100
Dallas district office	16	9	56	28	18	64
Des Moines district office	12	8	67	28	18	64
Detroit district office	32	32	100	25	7	28
Salt Lake City district office	5	5	100	17	9	53
	82	b/69	84	129	b/79	61

a/The Kansas City Security Administrator had submitted to the IRS national office some proposed changes to employee profiles and said that the national office had given oral approval to operate under these changes pending written authorization. Considering the proposed changes, 13 employee profiles still had unauthorized command codes.

b/The greatest number of unauthorized command codes for a single terminal was 15. The greatest number for an employee was 41.

Through these unauthorized command codes, users could access and make adjustments to tax data not required for performance of their duties. For example, one user possessed command codes allowing access to virtually any master file tax account even though the security manual stipulated that access for this user's position be limited to only those accounts presently on the service center system. In other instances, users had unauthorized command codes permitting them to release locked terminals, change employee profiles, and assign passwords.

IRS officials told us that the unauthorized command codes possibly resulted from the security manual being written in such a manner to define where work will be accomplished within the organization rather than leaving this to the director's prerogative. They also said that strict adherence to the manual would require organizational change.

Another cause for unauthorized command codes was security personnel failing to delete supplementary codes which the system automatically generated. A national office data retrieval system security official said IRS, subsequent to our review, researched those cases where the system automatically supplemented a primary code with others. As a result of its review, IRS either modified the computer program to discontinue the practice or the national office authorized the additional codes because a compromise of security was not involved. These changes should eliminate this problem.

IRS also changed the system to automatically delete an employee's profile when the new employee number indicates a change in organizational unit. This should prevent an employee from retaining unauthorized command codes when transferring from one unit to another.

Under present procedures, system security personnel, using security command codes in their profiles, input through a terminal the information necessary to make or remove an employee as an authorized user or add or delete command codes to or from an existing profile. In response to previous recommendations in our January 1977 report, IRS said it planned to automate the issuing of command codes. This change envisioned instantanecus establishment of an authorized profile, including the command codes necessary for performing the employee's duties. It would also centralize control over profiles and reduce or eliminate the need for many command codes now included in security personnel profiles.

National office officials say that IRS has since abandoned this plan because it did not take into account the various organizational alignments in service centers and districts. To recognize these organizational differences, they now plan to have each security administrator determine the content of each employee and each terminal profile subject to national office approval. The national office will, therefore, exercise control over profiles. The arrangement will also allow local management to exercise prerogatives concerning organization and workflow. But, national office officials will need to closely monitor whether local offices submit subsequent deviations for approval.

PROFILES OF FORMER RETRIEVAL SYSTEM USERS WERE NOT PROMPTLY DELETED FROM THE SYSTEM

Employees lose authority to use data retrieval system terminals due to reassignment, furlough, or termination. When these circumstances occur, IRS procedures require the security administrator to delete the related employee profile from the system but fail to specify a time frame for the deletion. Rather than deleting profiles on the effective date of the personnel actions, IRS takes days and sometimes weeks. This could provide an opportunity for unauthorized system use.

We sampled deleted profiles at service centers and districts and measured the time lapse between the employees' loss of authority and profile deletion. As shown below, security administrators did not delete profiles promptly.

Time Required to Delete Employee Profiles

	Number of profiles deleted							
Number of work days	Kansas City	Ogden	Dallas	Des Moines	Detroit	Salt Lake City	Total	Percent
1 or less	8	5	5	5	2	5	30	34
2 to 5	9	2	5	3	1	1	21	24
6 to 10	2	2	0	0	1	1	6	7
11 to 15	1	2	4	0	0	2	9	10
Over 15 (note a)	2	1	13	2	0	4	22	25
	22	12	27	10	4	13	88	100

a/Longest time was 30 weeks.

IRS procedures require security supervisors to notify the security administrator when a profile needs to be deleted. The delays in profile deletion occurred because supervisors did not prepare and submit notification forms in a timely manner.

Apparently, supervisors did not provide forms in a timely manner because no published IRS criteria exist on how promptly to delete a profile. It is essential for system security that deletions occur on the day of user termination, furlough, or reassignment.

One national office official said that he saw no problem with our asserted 1-day criteria. However, another said that deletion within one week would be more practical. He pointed out that delays are bound to occur because of service center size and the time required to prepare and process the necessary paperwork. He also said that security personnel may find it necessary to take care of more urgent matters. Considering this, he said that IRS expects to issue a revised manual in April 1977 providing a 5-day criteria for profile deletion.

While IRS met a 1-day criteria in only 34 percent of our sampled cases, we believe that it can generally accomplish all employee profile deletions on or before the effective date of the personnel action. The supervisor should know in advance when the action will occur, and the required notice form takes only a matter of minutes to prepare. The supervisor simply inserts the employee's name, organization, social security and employee numbers, and checks two blocks. It also takes little time for the security administrator to make the machine input necessary for profile deletion.

The other IRS argument advanced against a 1-day criteria pertains to the relative importance of the security administrator's profile deletion duties as opposed to other urgent matters. Placing the standard at 5 working days, while certainly an improvement over no criteria, may tend to play down the importance of immediately deleting profiles. To stress this importance, guidelines should require immediate deletion.

INADEQUATE CONTROL OVER RETRIEVAL SYSTEM SECURITY TAPES

IRS regulations require security over unassigned password listings and magnetic tapes containing authorized user names, social security numbers, and assigned passwords. This data needs security because someone obtaining it could access the system as though they were an authorized user. Notwithstanding, service centers did not properly secure some tapes containing this sensitive information.

While the Kansas City and Ogden service centers properly secured unassigned password listings, they did not adequately secure magnetic tapes containing authorized user names, social security numbers, and assigned passwords. For example, Ogden designated some retrieval system security tapes as available for general use and stored them in the tape library. Center personnel said the tapes had been erased but a printout showed they still contained sensitive data. At Kansas City, some retrieval system security tapes were duplicated and filed in the computer tape library--thus available to unauthorized personnel.

Center personnel did not prepare control records showing which tapes should be secured and who was authorized access to them. Only the security administrator needs access to the tapes, but the practices of both service centers gave potential access to programmers, analysts, and computer operators--those persons having the technical expertise to extract the taped data.

IRS has taken two steps to improve these conditions:

--Effective May 3, 1976, IRS, partially in response to problems we identified in our earlier review of its proposed computer system, started encrypting password data. Encryption will result in password data being unintelligible to an individual unless decoded.

--Effective June 10, 1976, IRS issued guidelines identifying the data retrieval system security tapes and listings requiring storage in a security cabinet. These guidelines also required the libraries to maintain a record showing who removed and returned security tapes and when.

These changes should make it more difficult to obtain readily useable password data and other sensitive information.

INADEQUATE PROTECTION OF THE RETRIEVAL SYSTEM SECURITY MANUAL COMPROMISES SYSTEM SECURITY

The security manual contains instructions for administering system security and describes system security features. Possession of the manual would allow a penetrator to study the system design for security flaws and devise a penetration plan. It also would aid an authorized system user in circumventing security controls. Even so, IRS did not adequately protect the manual.

Prior to June 1976, IRS guidelines did not specify protection requirements for the manual. In June 1976, however, IRS revised its physical and document security guidelines to incorporate Privacy Act requirements as well as to strengthen and expand existing security measures. These guidelines require that the security manual be protected not only by the user but during the preparation, printing, and distribution phases as well. The manual must now receive a level of security more than twice as great as that required for a tax return.

We evaluated security exercised over the manual both before and after issuance of the revised guidelines. During both periods, security was lax. Distribution control records failed to identify specific recipients and recipients failed to adequately protect the manual once received.

Tests at both the Kansas City and Ogden service centers prior to June 1976 showed that distribution records did not identify the individuals issued manuals. Through the security administrators, we identified individual recipients and observed the security being exercised. Thirteen (9 percent) of 141 manuals could not be located. In many instances, recipients stored the remaining manuals in or on a file cabinet or desk--places easily accessible by other personnel.

Tests at the national office during October 1976 showed that, despite the revised guidelines, IRS still exercised lax security over the manual. As in the service centers, distribution control records did not identify specific recipients. Sixteen (29 percent) of 55 distributed manuals could not be located. Eight of these 16 recipients said they had destroyed their manuals by shredding, tearing them up, or throwing them in the wastepaper basket, but did not document the disposition. Two more recipients said they returned their manuals to distribution personnel, but distribution personnel said they did not receive them. The other six recipients could offer no explanation as to what happened to their manuals.

IRS did not always coordinate distribution with need. Recipients of 11 (20 percent) manuals said they either had no need for the manual or received too many. Two of these recipients said they had unsuccessfully attempted to have their names removed from the distribution list.

National office recipients, as in the service centers, did not properly safeguard the manuals either during or after normal working hours. For example, during an after duty hours security inspection in October 1976, we found seven manuals on desk tops, in open bookshelves, or on radiator tops.

TRAINING FEATURES REDUCE SYSTEM SECURITY

Users of the data retrieval system access actual tax data for training purposes and can make training accesses whenever they choose. Because current procedures do not require a review of training accesses, system users are provided the opportunity to peruse many taxpayer accounts without challenge or detection.

Users learn how to use the system terminals through initial classroom instruction and subsequent on-the-job training. A system feature provides on-the-job training by allowing the user to access recorded data and, without actually changing it, practice making various transactions. The accessed data and the practice transactions appear on the terminal visual display screen. The production command codes in each user's employee and terminal profile limit the number and type of transactions that each employee may practice. This occurs because the system automatically matches each production command code with a corresponding training command code.

The system allows all users to make training accesses. The system record tape records both production and training accesses. An IRS official said a requirement exists for review personnel to evaluate user need for tax data accessed during production by reviewing selected transactions from the tape, but no requirement exists for a similar review of training accesses. Such a review could act as a deterrent against users browsing through recorded data not related to their assigned production workload.

IRS is currently developing a system modification to use fictitious rather than actual tax data for training purposes. If successful, this will eliminate the problem of using actual tax data for training. In the interim, however, IRS should expand its review of the system record tape to include training accesses.

CONCLUSIONS

The effectiveness of terminal and employee profiles depends on system security personnel following national office guidelines when giving and deleting user command codes. System users having unauthorized codes could make accesses and adjustments to tax data not needed to perform their assigned duties. Former authorized users could continue to access tax data until their profiles are deleted. Accordingly, security administrators must exercise caution against unauthorized command codes and promptly delete profiles when employees lose authority to use the system. Good system security dictates profile deletion no later than the effective date of termination, reassignment or furlough.

Good security also dictates that tapes and lists containing authorized user passwords and social security numbers be secured to prevent unauthorized personnel from accessing the system under the name of an authorized user. Near the end of our review, IRS began encrypting passwords and revised its guidelines for identifying and controlling security tapes. With proper implementation, these actions should improve tape security. IRS should determine whether these actions have been adequately implemented.

IRS should also recognize the importance of safeguarding the data retrieval system security manual. The manual could be very useful to an outsider or an authorized user in devising a scheme to circumvent security features. Improvement in present controls and safeguards over the manual is imperative.

The present system training features allow users unneeded access to actual tax data with little chance of detection. Through training codes, users can easily browse tax data not related to their assigned workload. While training is essential, it is not essential that training be accomplished with actual data. Until this problem is resolved, IRS should establish a review process for training accesses.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

To tighten security over the data retrieval system, we recommend that the Commissioner of Internal Revenue:

--Periodically assess whether security administrators submit employee profile changes for national office approval.

--Revise procedures to require that profiles of former operators be deleted within 1 workday after reassignment, furlough, or termination.

--Determine whether service centers have adequately implemented the June 1976 security tape control and accountability procedures.

--Establish a procedure whereby the system security manual is distributed only to those having a need for it; a record is maintained of the individual recipients; and proper disposition is made of unneeded or obsolete manuals.

--Require that recipients properly safeguard the security manuals.

--Develop and implement a retrieval system training module to preclude the use of actual tax data while training system users. In the interim, establish procedures requiring reviewers to spot check training accesses to see if the operator has a legitimate need to access particular taxpayer accounts.

IRS COMMENTS

IRS agreed with our recommendations and said that it has taken or plans to take corrective action (see app. I, pp. 76 to 78). Specifically, IRS said that it:

--Is establishing procedures allowing field offices to develop and maintain local employee profiles subject to national office review.

--Will contact each service center concerning the implementation of security tape control and accountability procedures and will review the continuing implementation through various review processes.

--Will establish procedures for distributing the system security manual and for maintaining a record of the individual recipients.

--Is developing a distinctive cover sheet for certain sensitive documents stating the protection required and will establish requirements to make recipients specifically accountable for the documents.

--Has implemented a system modification directing the bulk of training accesses to a training module containing fictitious tax account data.

IRS also said that it has issued new procedures requiring that former operator profiles be deleted as soon as possible but no later than 3 days after reassignment, furlough, or termination and will closely monitor the related compliance. While agreeing that a 1-day criteria could be met in most instances, IRS said that there may be some cases where more than 1 day would be needed. IRS' actions meet the intent of our recommendations.

CHAPTER 5

POLICY OF LIMITING ACCESS

TO TAX DATA NOT ENFORCED

IRS policy limits access to taxpayer data to those having a legitimate interest and a legal right. In other words, both third party and IRS employee accesses should be based on an official need to know.

IRS procedures implemented for third party accesses were, for the most part, adequate to carry out its policy. This is not the case, however, for accesses by IRS employees. Many employees gain access to data they do not need to do their jobs.

DISCLOSURE TO THIRD PARTIES

IRS can legally disclose tax data to third parties in certain circumstances. Before making such disclosures, IRS is responsible for determining that the request is in accordance with the law.

IRS discloses to third parties significant volumes of tax data in such forms as tax returns, microfilm or magnetic tapes. The following table shows some of the recipients and the volume disclosed in recent years.

Recipient	Number of disclosures on individual taxpayers		
	1974	1975	1976
States	58,911,922	62,980,779	65,855,434
U.S. attorneys	18,062	17,678	22,711
Department of Justice	10,446	11,485	9,505
Social Security Administration	6,633	5,835	5,484

IRS issued a handbook to guide its personnel in processing third party requests and delegated to field personnel the responsibility for reviewing and filling those considered as routine. Routine requests include data provided to State tax authorities and to the Social Security Administration for purposes of administering the Social Security Act.

Nonroutine requests require national office review and approval. Such requests include those from U.S. attorneys and most Federal agencies.

We reviewed IRS' procedures and examined the handling of selected third party requests at both the Kansas City and

Ogden service centers. While both service centers followed established procedures and denied improper requests, we noted one weakness in IRS' arrangement with certain States.

To obtain tax data from IRS, States are required to provide the cognizant district director, but not the service center director, with the names of State personnel authorized to request and receive the data and any subsequent authorization changes. Since States can deal directly with service centers, district directors are responsible for providing service center directors with the State's list of authorized recipients and any subsequent name changes.

For those States authorized to receive data from the Ogden and Kansas City service centers, we obtained current lists of authorized personnel and compared them with the lists being used by the service centers. The centers' lists contained only personnel authorized by all but one of the States. The Kansas City center's list contained five names not on this State's list.

The State reported removal of these authorizations to the district director on March 24, 1976. But the district director did not report these changes to the service center until August 13, 1976. Thus, for a period of about 5 months, these five people could have continued to request and receive tax data without authorization. This situation could have been avoided if IRS required the States to simultaneously provide district and service center directors with authorization lists and any subsequent changes.

DISCLOSURES WITHIN IRS

IRS policy provides that employees can be furnished tax returns and tax data only when needed to perform official duties. Although IRS established procedures to carry out this policy, its failure to implement and monitor some of them weakened their effectiveness and some employees received unneeded tax data.

Controls to limit access to only authorized personnel

As one means of limiting access to those having a reed to know, IRS designates certain areas as restricted. Guidelines specify that entry to these areas be limited to authorized personnel. Restricted areas are to be prominently posted and physically separated from nonrestricted areas. The number of entrances are to be limited and controlled by positioning a responsible employee to make certain that only authorized persons enter. Persons having a limited need to be in the area are to sign an in and out register.

Most locations visited assigned personnel to monitor movement in and out of restricted areas. In some high volume areas, an electronic signal alerted the monitoring personnel when a person entered or left the area. However, some monitoring personnel said that they never challenged anyone's need for entry.

Most monitoring personnel also maintained sign-in/sign-out registers. In accordance with IRS guidelines, all registers showed who entered, entry time and exit time. However, the guidelines do not require other descriptive data, such as the person to be contacted and the purpose for the entry. Although the registers were available, management officials did not review them to determine who entered the area and why, and to evaluate the need for entry.

IRS uses special color coded badges to identify those employees and visitors authorized to be in a restricted area. Different colored badges distinguish between areas.

Two problems occurred in the badge process at the National Computer Center. First, the center issued visitors the same color badges as are worn by IRS employees assigned to restricted areas. To control visitor movement into and within restricted areas and to permit ready identification, the center should issue them a distinguishable badge as well as require them to sign in and out of the area.

The second problem, while extensive at only the National Computer Center, also occurred to a lesser extent at another installation. Center officials determined that all its employees and 366 of 559 vendor personnel had a need for free access to one or more restricted areas. To a lesser extent numerous designations also occurred at the Salt Lake City district office which granted 71 of its 209 employees access to one microfilm room. Such extensive free access largely defeats the purpose for establishing restricted areas.

Controls over employee requests for tax data

In some instances, IRS adequately determined that an official need for employee-requested tax data existed. In other instances, the procedures were weak or nonexistent and IRS personnel received unneeded tax data.

IRS procedures specify that supervisors must review the need for tax data requested, approve each request before it is filled, receive the requested data, and give it to the requester. We reviewed the practice of selected supervisors at the two service centers and four district offices. The amount of control varied according to what each supervisor thought was necessary. Some performed no review.

Neither service center nor district supervisors routinely review all requests for tax data. For example, supervisors at both the Dallas and Salt Lake City districts review all requests for returns, but Dallas supervisors do not review any requests for microfilm. Salt Lake City supervisors in one organizational unit review microfilm requests but not in another. At Kansas City, we interviewed seven supervisors in charge of units that routinely request tax data. All seven said they neither review all requests nor require that requested data be routed back through them. Their practices included one or more of the following:

--Using request forms containing pre-stamped supervisory approval.

--Allowing requesters to sign for them.

--Spotchecking requests for a need to know.

--Relying on knowledge of cases being worked.

No supervisors controlled data retrieval system user requests; rather, they relied on the safeguards built into the system. These safeguards were previously discussed on pages 22 to 23.

Tests of need to know

To test the requester's need to know, we intercepted various types of requested tax data, delivered it to the requesters, and discussed with them why the data was needed. The test included tax returns, master file computer transcripts, data retrieval system printouts, and microfilm transcripts.

A computer transcript is a printout of the account data recorded in the master file. Data retrieval system printouts show whatever data is displayed on the terminal screen. Microfilm transcripts include:

--Name directories which show a taxpayer's name, social security number, and tax periods for which a return was filed.

--Account registers which show the transactions in a taxpayer's account by tax period for open accounts maintained on the master file.

--Retention registers which show the transactions in taxpayers accounts that have been removed from the master file because of inactivity.

Our combined results for the national office, two service centers, and four district offices showed that in each instance the subject taxpayer was part of the requester's assigned workload and that in 95 percent of the tested requests the requester needed all or some of the data. The following table shows the test results by request type.

	Requests for					
	Returns	Microfilm transcripts	Computer transcripts	System printout	Total	Percent
Tested	153	134	95	54	436	100
Not needed	4	1	13	2	20	a/ 5

a/All but one of the totally unneeded requests occurred at the service centers.

Primary reasons for obtaining unneeded data appear to be

--procedural guidelines and supervisory instructions designed to expedite completion of assigned work and

--failure to evaluate data needs.

Both reasons result in a "If you think you might need it, request it" attitude. For example, one employee, in accordance with written instructions, ordered both a transcript and a return. Using the transcript, the employee completed the work before receiving the return. When we delivered the return, he said it was not needed and that this happens frequently. Personnel in one organizational unit said they ordered all available data in order to meet management's deadline for completing work on each case.

Some personnel requesting computer transcripts did not properly evaluate data needs. A requester can order a computer transcript for one or more tax periods, such as for an individual's 1975 form 1040, or order a complete transcript showing all data on the master file for that particular taxpayer. Complete transcripts may, therefore, show a considerable volume of unneeded data. For example, in a case relating only to employment taxes, the requester ordered a complete business master file transcript. In addition to receiving the needed employment tax data, the requester received data on the taxpayer's Federal excise taxes for the years 1968 through 1975 and income taxes for the period 1968 though 1976.

Although most microfilm transcript requests were for needed data, the requesters also obtained significant amounts of unneeded data on other taxpayers. For 134 requests reviewed, the transcripts showed tax data on 2,197 other taxpayers. This occurred because the equipment used to make the transcript cannot print the information for just one taxpayer. The equipment vendor for the Kansas City service center knew of no commercially available equipment that could.

Although equipment shortcomings exist, IRS could reduce the volume of unneeded data provided via microfilm transcripts. Contrary to guidelines, requesters in many cases ordered a complete transcript when they only needed limited data--for example, the taxpayer's social security number or verification of name and address. In other cases, microfilm researchers provided a transcript when the requester only asked for limited data. For example, of 50 Kansas City requests, 14 transcripts were ordered although only limited data was needed and four transcripts were furnished although only limited data was ordered. Had the microfilm researchers recorded the needed data on the request form and returned it instead of providing transcripts in these 18 cases, the requesters would not have received unneeded data on 284 other taxpayers.

Another alternative is to obliterate or remove the unneeded data from the transcripts. IRS now uses such a procedure to limit access in some cases. While such a procedure requires additional manpower, it may be the only way to completely limit microfilm access to needed data until related equipment is commercially available.

DOCUMENTATION OF ACCESSES

The Privacy Act of 1974 requires IRS to record certain third party accesses to individual's tax returns and tax data. It does not require IRS to document employee accesses made in the course of their official duties.

To carry out the Privacy Act intent, IRS implemented procedures on September 27, 1975, for manually documenting third party accesses. On January 16, 1976, IRS made its computerized accounting system for third party accesses fully operational. Since the system was being developed and implemented during our review, we did not completely test it. Limited tests, however, indicated that IRS prepared the required documentation.

Although not legally required, IRS documents some employee accesses of tax returns and tax data. Effective March 1975, IRS started documenting employee requests for processed returns. At the Commissioner's direction, service centers and Federal Records Centers started keeping a copy of written employee requests for (1) tax returns, (2) information from tax returns, and (3) photocopies of returns. IRS also documents employee accesses of tax data in the data retrieval system by means of a tape record showing transactions processed and accounts accessed by each user.

IRS employees make millions of other accesses which are not documented. For example, Kansas City service center employees who process tax returns when they are initially received have potential access to about 13 million returns annually. Each return must go through at least five and possibly as many as nine steps to convert it to a machine processable format. This is called the "pipeline" and IRS does not attempt to document these employee accesses. Neither does IRS attempt to record employee microfilm and computer transcript accesses. About 15.8 million microfilm and 12.5 million master file transcript requests were filled in 1976.

Since IRS is not legally required to document employee accesses, we did not attempt to evaluate its voluntary practices in this regard. IRS officials stated, however, that documenting all employee accesses, or even as many as possible, would be an administrative burden, would decrease efficiency, and would substantially increase the cost of operations.

CONCLUSIONS

IRS attempts to protect tax data confidentiality by limiting third party and employee accesses to those who have a legal right and an official need to know. In this respect, IRS has effectively implemented its procedures and controls pertaining to third parties. It has not, however, effectively implemented those applicable to IRS employees. IRS employees should have no special rights to access tax data except when performing official duties. We recognize the need to expedite production, but to better protect tax data confidentiality, IRS should limit the current level of employee access.

On the basis of our limited tests, IRS appears to satisfactorily meet the legal requirements for documenting accesses. While we did not determine whether IRS should attempt to document additional employee accesses, we recognize the impracticality of trying to document them all, especially those occurring during initial service center processing.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

To meet IRS' policy of limiting taxpayer data to only those with a legitimate interest and a legal right, we recommend that the Commissioner of Internal Revenue:

--Amend agreements with States to require that both the cognizant service center and district directors be simultaneously provided the lists of State representatives authorized to request tax data and any subsequent changes to the lists.

--Reemphasize the importance of limiting restricted area access to only those having an official need by requiring responsible officials to reevaluate and document the reasons why so many people have been granted access.

--Establish procedures requiring that districts restrict microfilm room access to only a few designated employees and that these employees fill only written requests.

--Revise restricted area sign-in/sign-out register format to show the person to be contacted and the purpose for entry; and establish procedures for reviewing the registers to determine who entered the area and the need for entry.

--Revise guidelines to require that supervisors either review and approve requests for tax data or use a valid sampling plan to spotcheck tax data in possession of employees to determine that only needed data is being obtained.

--Revise procedures to require that microfilm researchers fill requests for limited data by recording it on and then returning the request form rather than providing a complete transcript.

--Consider alternatives for eliminating from microfilm transcripts all data not pertaining to the taxpayer that is the subject of the request.

IRS COMMENTS

IRS agreed with our recommendations and said that it has taken or plans to take action in each instance (see app. I, pp. 78 to 80). Specifically, IRS said that it:

--Will notify State tax agencies by letter to provide lists of authorized State representatives simultaneously to service center and district directors and will subsequently revise its related agreement form as well as pertinent publications to include this requirement.

--Will reemphasize the importance of restricted area controls, review the appropriateness of existing restricted area designations as well as the need for such designations over other critical operations, continue ongoing tests of computer-controlled entry to restricted areas, revise sign-in/sign-out registers as recommended, and require that the registers be periodically reviewed.

--Will issue instructions requiring district office microfilm personnel to honor only written requests and consider revising procedures to require that requests for limited data be filled by transcribing the data on the request form.

--Is testing an equipment modification to limit the number of taxpayers whose tax data appears on a microfilm transcript and will require that replacement equipment be able to limit data to a specific taxpayer.

--Will reemphasize the need for supervisory review of data requests and will reevaluate existing guidelines in terms of possible revision to include alternative approaches where the volume of data requests prohibit a 100 percent supervisory review.

CHAPTER 6

BACKGROUND INVESTIGATIONS NOT BEING EFFECTIVELY UTILIZED

IRS relies heavily on the integrity of its employees and others, such as contract guards and janitors, to prevent unauthorized disclosure of taxpayer data. Recognizing this, IRS requires that each employee receive a background investigation. Under contract terms, contract personnel are to submit background information to the Civil Service Commission or the General Services Administration.

Notwithstanding the heavy reliance on employee integrity and the related emphasis on background investigations, IRS assumes the risk of permitting employees to work pending receipt of background investigation results. Certain IRS practices greatly magnify this risk, such as

--initiating or performing investigations in an untimely manner,

--assigning employees to sensitive positions without initiating or performing investigations, and

--failing to determine whether contract personnel received an investigation.

BACKGROUND INVESTIGATIONS: APPROACH AND RESULTS

IRS designates each position as nonspecified, specified, or critical-sensitive depending on the degree of adverse effect the occupant could cause to national security, such as a revenue agent conducting an audit on a firm that does defense contract work, or the degree of trust inherent in the position. The following table shows the type of investigation required and the investigating agency for each type of position.

Type of position	Type of investigation required	Conducted by
Nonspecified (note a)	National Agency Check and Inquiry	Civil Service Commission
Specified (note a)	Character investigation	IRS Assistant Commissioner for Inspection

Type of position	Type of investigation required	Conducted by
Critical-sensitive	Security investigation	IRS Assistant Commissioner for Inspection

a/Although a temporary employee hired through a 90-day or less appointment may be placed in a specified or nonspecified position, IRS guidelines require only a check of local police records rather than the more extensive background investigation required for other employees.

The scope of these investigations vary. A National Agency Check and Inquiry includes a check of Federal Bureau of Investigation, Civil Service Commission, military and other Government agency records, and written inquiries to former employers and supervisors. Being more comprehensive than a National Agency Check and Inquiry, a character investigation includes personal interviews and covers the shorter period of either the last 10 years or from the person's eighteenth birthday to the date of the investigation request. The character investigation generally includes personal interviews with former employers, supervisors, co-workers, references, neighbors, and others. It also includes summaries of any previous investigations; police and credit checks; verification of education; and inquiries concerning the person's character, reputation, and loyalty. A security investigation, the most comprehensive, covers the shorter period of either the last 15 years or from the person's eighteenth birthday to the date of the investigation request. It consists of a check with the Federal Bureau of Investigation, the Civil Service Commission, the appropriate military department, and contacts with former employers and supervisors, references, and schools.

Available statistics for character investigations performed by IRS show that:

Fiscal year	Number of IRS investigations	Employees with unfavorable investigation results	Released from employment as a result of investigation
1974	13,823	488	102
1975	11,104	490	96
1976	10,291	381	94

According to IRS, various factors that could result in an unfavorable determination include:

1. False statements on application papers.

2. Omission of items, such as adverse employment history, on application papers.

3. Misrepresentation of facts on application papers.

4. Poor reliability and trustworthiness in past performances.

5. Criminal records not disclosed on application papers.

6. Dishonest, immoral, or disgraceful acts.

7. Derogatory income tax information.

As shown in the preceding table, an unfavorable determination does not always result in release from employment. IRS officials said that some employees with unfavorable determinations were still employed but had received disciplinary actions, such as suspension, reprimand, or demotion.

NOT ALL IRS EMPLOYEES HAD RECEIVED REQUIRED BACKGROUND INVESTIGATIONS

IRS, through administrative oversight, failed to initiate the required background investigation for some employees. Lack of a follow-up procedure for initiated investigations contributed to some employees occupying nonspecified and specified positions for extended periods before investigation results were available.

To ascertain whether IRS obtained the required level of background investigations on its employees, we selected 811 from the total of about 17,000 positions at all locations visited. Preliminary testing disclosed two problems.

First, IRS had not initiated a request for the proper level investigation for 25 employees. IRS guidelines provide that a request for a National Agency Check and Inquiry should be made within 3 days of the appointment. Although the guidelines do not specify a similar criteria for initiating a character investigation, the same time requirement should apply. In these 25 cases, the employees received the appointments to their present positions from 2 weeks to about 13 years before the date of our review. Two cases pertained to initial appointments and the remaining 23 pertained to cases where the employee's present position required a more comprehensive investigation.

The second problem related to the amount of time required to complete an investigation. IRS guidelines do not establish a time goal for completing investigations or for following-up when investigation results are not received timely. One national office official said IRS' goal is to complete investigations within 9 months and another said IRS was considering whether to lower the goal to 6 months.

Although all 811 sampled cases were not checked for this attribute because many investigations were conducted in years past, we noted 7 cases where the investigation had been requested 9 months or more previously. For these cases, the elapsed time between the date of the request and our review ranged from 9 months to 15 months. One of these cases involved a position in a regional office Intelligence Division where the employee's clearance was denied about 10 months after the investigation had been requested. Consequently, IRS planned to terminate the employee.

A review by the Office of the Assistant Secretary (Administration), Department of the Treasury, disclosed similar problems with IRS background investigations. In its July 1972 report, "A Study Of Personnel Security Clearance Procedures," Treasury attributed the failure to timely receive requested background investigation results to reasons such as

--applicants failing to fill out forms properly,

--hiring offices not following the deadlines for initiating investigations,

--unidentifiable fingerprints delaying the Federal Bureau of Investigation identification process,

--time taken by the Civil Service Commission to complete investigations,

--character investigations conducted by IRS not taking top priority over some other type investigations, and

--difficulties encountered by investigating agents in getting people to disclose information.

On a limited basis, we expanded our tests to see how extensive the problem might be or whether the timeliness of these actions had improved. At the Detroit district and Detroit data center we selected 70 cases involving recent hires and promotions.

The following table shows that while differences exist between locations, neither location approached meeting the 3-day criteria for initiating investigation requests.

	Number of cases			
Time (days)	Detroit district	Detroit data center	Total	Percent
3 or less	11	3	14	20
4 to 9	9	2	11	16
10 to 15	0	4	4	6
16 to 45	1	14	15	21
46 to 60	1	9	10	14
61 to 75	0	2	2	3
76 to 90	0	2	2	3
Over 90	0	12	12	17
Total	22	48	70	100

The Detroit district met the 3-day goal in 11 of 22 cases (50 percent) while the data center met it in 3 of 48 (6 percent). Detroit district and data center officials attributed the failure to timely request investigations to unavailability of staff, and to large numbers of persons being hired at one time, thus overburdening the existing staff.

Another limited test showed that there had been little improvement in the time required to receive investigation results. A test of 120 pending investigations of Ogden data retrieval system users showed that 14 (about 12 percent) had been pending for more than a year.

Because it places employees in positions pending receipt of a favorable background investigation, IRS needs to initiate investigation requests within the required 3 days. IRS also needs to periodically follow up on requested investigations to obtain the results as soon as possible.

TEMPORARY EMPLOYEES ASSIGNED TO SENSITIVE POSITIONS

IRS installations use 90-day or less temporary appointees in both specified and nonspecified positions, usually during the peak workload season. Although IRS guidelines require that occupants of specified positions receive a character investigation, temporary employees receive only a police check.

Notwithstanding the limited background investigations, the Kansas City service center during one peak workload period placed 192 temporary employees in specified positions. This practice increases the chances of placing untrustworthy employees in positions providing access to large volumes of tax data which thereby increases the possibility of an unauthorized disclosure.

While IRS guidelines permit placing temporary employees in specified positions, we believe the practice is contrary to the intent of establishing required security levels for sensitive positions.

BACKGROUND INVESTIGATIONS ON NON-GOVERNMENT PERSONNEL

Several thousand non-Government personnel work in IRS installations, some on a daily basis. For example, 281 and 278 non-Government personnel work in the Kansas City and Ogden service centers, respectively. About 560 non-Government personnel are authorized entry at the National Computer Center. Employees of at least 24 companies work in the Detroit district office. These non-Government workers provide a wide range of services, such as guard, janitorial and food (cafeteria) service, office machine and computer service, vending machine service, and gardening services.

Presently, IRS performs no background investigations on non-Government personnel who routinely work at IRS installations. While most work is performed during normal duty hours in the presence of IRS employees, some non-Government personnel have access to most areas of the facility both during and after normal duty hours, especially guards and janitors.

Guards and janitors have a great degree of freedom of movement throughout the installations. For example, the contract guards at the Kansas City service center routinely patrol the building after normal duty hours and are given keys allowing entrance into all areas, including the microfilm room and return file room. IRS requires some areas to be cleaned during duty hours in the presence of IRS employees while janitors may clean other areas after normal duty hours or without the presence of an IRS employee. Some of these areas contain unsecured tax data, including tax returns.

According to a General Services Administration official, guards and janitors employed under General Services Administration contracts receive a background investigation. These contracts require that background investigation data be provided to the General Services Administration or the Civil Service Commission. However, IRS officials had not attempted to ascertain whether the data had been provided or the investigation performed.

IRS management recognizes the risk posed by guards and janitors but questions whether it has legal authority to make background investigations on non-Government personnel. In response to our January 1977 report, IRS said that it would consider the legality of performing its own background investigation of these contract personnel. [1]

CONCLUSIONS

IRS takes considerable risk of unauthorized tax data disclosure by assigning employees to sensitive positions before obtaining background investigation results. Guards, janitors, and other non-IRS employees pose a similar risk.

IRS could reduce the present level of risk and thereby significantly improve security over taxpayer data by:

--Instituting controls to make certain that background investigations are requested promptly and completed to the extent possible within the IRS goal of 9 months. The 6-month completion goal now under consideration by IRS would even further reduce the present level of risk.

--Following up to determine that the many non-Government employees working within IRS installations receive a background investigation.

[1] "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration," LCD-76-115, Jan. 17, 1977.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

To improve the present level of security provided through background investigations, we recommend that the Commissioner of Internal Revenue:

--Specify a 3-day criteria for requesting all background investigations.

--Establish control systems for monitoring compliance in meeting the 3-day and 9-month goals for requesting and completing background investigations. As a minimum, the control systems established should provide for periodic followup action, identification of instances where the goals are exceeded, and management reports explaining the reasons why the goals were not met.

--Establish procedures requiring local management to ascertain the results of background investigations conducted by other agencies on non-Government personnel who work in IRS facilities.

IRS COMMENTS

IRS agreed with our recommendations and said that it has taken or plans to take corrective actions (see app. I, pp. 80 to 81). Specifically, IRS said it:

--Is establishing additional control systems for more effective background investigation case management such as a computerized information system to provide periodic data on initiation and completion of background investigations, and a monthly case aging report to use in monitoring all overage cases.

--Will ask the General Services Administration to furnish local IRS management with the results of background investigations on non-Government personnel, such as guards, janitors, and cafeteria employees who work in IRS facilities.

--Will include requirements for background checks in its own contracts and explore the feasibility of doing the same in leasing agreements.

IRS also said that it will ask the General Services Administration for authority to award its own major contracts such as those for guard and cleaning services. Should the request be denied, IRS said it will seek related legislation.

IRS said it has recently revised its requirements to specify that background investigations must be requested within 1 week of the employee's entrance on duty. This criteria meets the intent of our recommendation.

CHAPTER 7

WEAKNESSES IN PHYSICAL SECURITY PRECLUDE MAXIMUM PROTECTION

The physical features of IRS facilities are adequate to deter general access by unauthorized persons. However, badge system weaknesses could make it easy for someone to enter a facility and possibly obtain unauthorized tax data.

Other threats to tax data confidentiality result from IRS permitting guard and janitor access to large quantities of data; personnel not obtaining receipts for tax data shipped through the mail; and microfilm custodians not establishing accountability controls over microfilm records containing data on thousands of taxpayers.

Most of these threats have resulted from the failure of assigned personnel to monitor compliance with prescribed procedures and controls.

FACILITIES AND GUARD SERVICE

IRS uses various physical features to secure its facilities. The features used depend on the building type, occupants, neighborhood, nature of operations conducted, necessity for public access, and types and quantity of tax data in the building.

IRS has established physical feature requirements for its national office, the National Computer Center, the data center, and service centers. As required, the national office used a uniformed security guard service and locked exterior doors during nonwork hours. The National Computer Center, the data center, and the two service centers visited each complied with requirements by using

--a uniformed security guard service on duty 24 hours a day,

--an electronic intrusion detection system monitored by the guards, and

--a perimeter fence.

IRS guidelines for regional and district offices are more general in terms of required physical features. The regional and district offices visited secured their facilities by using locked exterior doors during nonwork hours and either full-time or part-time security guards. At district post-of-duty offices, a locked building and locked file cabinets provided the basic nonwork-hours security.

IRS facility features and the guard service seem adequate to control general access.

WEAK IMPLEMENTATION OF THE BADGE SYSTEM

On a given day, several thousand employees and numerous visitors may enter an IRS facility. IRS uses a badge system at service centers, the National Computer Center, and the data center to identify, permit entry, and control the movement of authorized personnel and visitors.

IRS regulations require every employee or visitor to wear a standardized, serially numbered, color-coded, laminated badge. IRS employees and non-IRS personnel who regularly work at a facility wear badges displaying their photographs. Occasional visitors wear badges without photographs. A badge's color signifies the area(s) to which the wearer has been authorized access and whether the wearer is an IRS or non-IRS employee. Regulations require non-IRS personnel to surrender their badges when leaving a facility, and employees to surrender their badges when furloughed for more than 2 weeks or when terminated.

Our review showed that the badge system's effectiveness in safeguarding tax data was reduced because

--some non-IRS personnel received the same color badges as IRS employees,

--all employees and most visitors at the National Computer Center received badges authorizing them access to restricted areas (see p. 39), and

--some facilities did not properly control and account for badges.

Non-IRS personnel receive the same color badges as IRS employees

The facilities issue some non-IRS personnel the same color badges as are issued to IRS employees. Although permissible under existing procedures, this practice results in non-IRS personnel not being readily distinguishable from IRS employees. The following table shows the extent of this practice by facility and type personnel.

	Number of badges			
Types of non-IRS employees	Ogden Service Center	Kansas City Service Center	National Computer Center	Detroit Data Center
Contract guards	35	23	0	27
Federal Protective Service guards	5	0	13	0
General Service Administration building management personnel	18	46	0	0
Federal Records Center employees	0	31	0	0
State Tax Commission representatives	4	0	0	0
Vendors	0	0	558	0
Retired IRS employees	2	0	0	0
Total non IRS employees who had the same colored badge as IRS employees	64	100	571	27

Since the badges are the same color as those worn by IRS employees, the non-IRS personnel can not be readily identified. While some non-IRS personnel may normally wear a distinguishing uniform, they could easily gain access to the facility while wearing regular clothing. The badges indicate that these non-IRS personnel have the same rights and privileges as IRS employees with the same color badges.

Badges not properly accounted for, controlled, or verified

IRS did not properly account for or control badges because it did not fully implement or enforce established procedures. Failure to properly control and verify badges increases the chance of an unauthorized person gaining entrance to the facility.

Adequate badge control necessitates records of who has which badge. Recognizing this, IRS procedures provide that two records be maintained to identify authorized badge holders and authorized badges. One of these records shows the badge holder in badge numerical sequence; the other shows the badge holder and his number in alphabetical sequence. IRS procedure requires an annual audit and reconciliation of these two records.

Service center practice, however, was to compare one record to the other, and determine whether they agreed. This practice does not assure that a badge holder actually has the recorded badge. To effectively control badges, IRS must

--keep the records current and annotate all changes,

--reconcile records periodically, and

--verify the accuracy of the records by tracing at least a sample of badges to the badge holders.

The service centers had fully implemented their present badge system by August 1975. In January 1976 we tested badge controls at Kansas City. Verification of badge records and badges worn by 54 of 2,790 employees showed that

--in 48 instances, the badge holder wore the correct badge;

--in 3 instances, the badge holder wore a different badge number than shown by the numerical control register;

--in 1 instance, the badge holder wore a badge with a different color and number than that shown in the control register; and

--in 2 instances, the badge unit kept badges of former employees rather than destroying them as required.

Another limited test disclosed other errors such as

--the alphabetical record showing seven badges of terminated employees as destroyed while the numerical record showed them as active,

--the alphabetical record showing one badge as lost while the numerical record showed it as active, and

--both badge records showing one badge as active although a terminated employee reported it lost.

These errors resulted because responsible personnel did not keep current one or both of the badge records. Reconciliation of the records would have disclosed most of the errors. However, to provide greater assurance that badges are effectively controlled, badge unit personnel must also compare the records with the badges actually held. IRS guidelines do not require such a procedure.

Authenticity checks were not being made

Periodic badge authenticity checks could serve as an effective measure to detect and deter the use of false badges. IRS procedures require authenticity checks at some installations but not others. Even where required, the checks were not being made.

Service centers are required to perform semiannual authenticity checks which consist of illuminating a special insignia on the badge with a special light. The Kansas City and Ogden service centers did not perform these checks because both facilities lacked the necessary equipment. According to IRS officials, the National Computer Center and the data center were exempt from the requirement because their badges had not been reissued using the new material.

At all installations using badges, guards monitor entrances to determine that people entering wear a badge. However, the guards generally do not compare the photograph on the badge with the wearer, particularly during work shift changes. Therefore, a person using a false badge or an authentic badge of another person could easily enter the building.

This happened at the Detroit data center when an employee loaned his badge to an outsider who used it to enter the facility. The guards detected the unauthorized person in the building at about 3:00 a.m. but did not know when he entered or where he had gone in the building. The data center fired the employee for loaning his badge.

Periodic authenticity tests and periodic matching of badges and badge holders may not have prevented the above incident; however, they would act as a deterrent and thereby help reduce the threat of unauthorized persons gaining entrance. IRS should require authenticity checks at all badge-using facilities.

New badge system is being developed

Recognizing the need for a stronger badge system, IRS officials started testing a new one at the Cincinnati service center in July 1976. In fiscal year 1979 IRS plans to implement a servicewide identification system using a combination identification card and badge. The planned system includes a computerized badge reader which will electronically control access to buildings, restricted areas, and computer terminals. It will also test authenticity each time a card is used.

The new system offers no panacea for the present system's weaknesses. Under both systems, badges must permit visual identification of visitors; management must judiciously issue restricted area badges; and control personnel must maintain current and accurate badge records. Related weaknesses in the present system, if not corrected, will reduce the new system's effectiveness.

PHYSICAL PROTECTION OF TAX DATA

The protective point value system

Locked containers, vaults, locked rooms, locked buildings, and guards are used to protect tax data during nonwork hours. Because installations use various combinations of these features, IRS officials developed uniform protection requirements for documents and other items by assigning them numerical values. The numerical value assigned directly relates to the amount of physical protection a document or item needs--the higher the number, the greater the protection needed. For example, a tax return requires three point protection; microfilm requires six points.

IRS also assigns numerical values to containers, areas, and certain installations in direct relationship to the protection they afford. For example, certain locked metal file cabinets provide 3 point protection, a vault provides 30 points, and service center physical features provide 4 points. The containers and areas may be used in combinations. For instance, a locked file cabinet (three points) located within a service center (four points) provides a document seven protection points.

Guards and janitors have ready access to tax data after work hours

IRS, in implementing the protective point system, considered threats from the general public as well as from some internal sources. But throughout the Service, IRS accepts the threat posed by guards and janitors. IRS officials cite a Chief Counsel's opinion issued in 1966 and reaffirmed in 1976 as the reason. The IRS Chief Counsel concluded:

> "* * * that policing and cleaning personnel may be granted access to spaces containing tax returns in order to perform their duties and that granting of such access would not violate the provisions of the disclosure statutes."

Guards and janitors work in IRS office space after normal work hours. We made after-hours tours of selected facilities during 1976 and found tax data readily accessible or in plain view at the national office, regional offices, district offices, service centers, and the data center.

For example, data center personnel stored tax returns on open shelves in open work areas. Detroit district office personnel left audit case files and tax returns on desk tops. Des Moines district office personnel stored tax returns and audit case files in unlocked containers and left on a desk top a list of individuals having large delinquent tax liabilities. National office personnel left numerous documents, including corporate returns, computer printouts, and a 1970 study of the net worth of 55 millionaires in plain view.

Placing tax data in locked containers, while unfeasible at some locations, could eliminate accessibility; but, IRS' protective point system does not require this degree of protection. For example, service center audit case files and related correspondence placed in any unlocked container are considered adequately protected because of the protection points assigned to the facility's physical features. At the district offices visited, IRS considers tax returns protected even if left on desks, table tops, or in unlocked containers because of the protection points assigned to a locked and guarded building.

Accessibility risks could also be reduced if all cleaning was performed only in the presence of IRS employees. This is now required for restricted areas. However, IRS officials said that it is not always possible to arrange all cleaning schedules to coincide with IRS duty hours.

To better protect tax data confidentiality, IRS needs to further consider the threats posed by non-IRS personnel having access when IRS employees are not present and secure the data when volume permits or otherwise alleviate its accessibility.

Closer monitoring of the protective point value system is needed

Weaknesses in physical and document security occurred because security personnel did not perform their assigned monitoring responsibilities. National office officials responsible for IRS' overall physical and document security program had not undertaken any compliance monitoring activities and local security personnel were not performing required facility inspections.

The national office, regional and district offices, service centers, and computer centers each have a protective programs manager or officer responsible for implementing and monitoring the protective point value system. Assigned responsibilities include performing annual facility inspections to determine the adequacy of security and reporting the inspection results to management. Of the facilities visited, only officials at the Des Moines district office, Chicago regional office, and data center complied with the inspection and reporting requirements.

One aspect of the required inspection pertains to determining whether secured areas have been established where necessary. However, the Kansas City and Ogden service centers had secured area doors without proper locks. Local managers did not know about these security deficiencies because the local protective program officers had not carried out the assigned monitoring and reporting duties.

Local officials have been made aware of some weaknesses in the security program through various reports issued by IRS' Internal Audit Division. However, an Internal Audit official said that internal audits are not substitutes for compliance monitoring by responsible security managers.

A national office official responsible for physical and document security attributed the widespread lack of monitoring to management's failure to place proper emphasis on security, and lack of a formal security-oriented training program.

Tax data shipments haphazardly controlled

IRS guidelines require that the sender of tax data receive a receipt confirmation within a specified period. If the confirmation is not received, procedures require the sender to follow-up with the intended recipient. Receipt confirmations were not being received and the required followups were not being made.

IRS routinely ships tax returns, microfilm, and magnetic tapes containing taxpayer data via the U.S. Postal System between IRS locations and to other Federal agencies such as the Social Security Administration.

Procedures require that a transmittal document accompany the shipments and that recipients verify the shipment contents and acknowledge receipt by returning a signed copy of the transmittal document. The sender should maintain a file of unacknowledged transmittal documents to alert him when to make a followup. Acknowledgement should occur within a specified time period, 7 to 15 workdays, depending on the type of data transmitted.

At all locations visited, except the Detroit district office, recipients did not consistently acknowledge shipments and senders did not consistently take followup action. For selected shipments, the intended recipient had not acknowledged receipt in 2,356 cases. The number of unacknowledged shipments varied between locations and ranged from 7 of 965 shipments at the National Computer Center to 1,248 of 27,239 shipments at the data center. Shipments remained unacknowledged for periods ranging from 12 to 103 workdays.

By failing to implement prescribed procedures, IRS is relying on a complaint system for identifying unreceived shipments. However, many recipients are not notified to expect shipments and, therefore, would not know to complain if a shipment were not received. Considering the volume of shipments and the type data shipped, reliance on a complaint system is unsatisfactory.

Accountability for microfilm records not established

Many IRS offices use microfilm containing tax liability and payment data identified by taxpayer. The microfilm provides large volumes of concentrated, indexed and cataloged data on portable and easily pilferable cartridges. A single microfilm cartridge, measuring about 3" X 5" X 1", may contain data on as many as 2,200 taxpayers. The number of cartridges on hand varies between IRS facilities. For example, at the time of our review the Ogden service center had about 27,000 cartridges containing tax data on about 13,500,000 taxpayers and the Salt Lake City district office had about 1,400 cartridges containing tax data on about 800,000 taxpayers.

IRS guidelines require records showing microfilm received, produced, reproduced, transmitted, destroyed, and the dates of these actions. Guidelines also require quarterly physical inventories.

Notwithstanding these guidelines, only one of the installations visited maintained records which could be used to establish accountability and identify missing microfilm. Most did not take the required quarterly inventories. When taken, results were not used to confirm the accuracy of the records. For example, three custodians took inventories--two for the sole purpose of establishing space requirements. The other custodian said that he used the inventory results to adjust records showing the total number of cartridges on hand, but could provide no documentation showing the inventory results or the adjustments made.

We took physical inventories of microfilm at the Dallas district office and noted several discrepancies. For example, one custodian was missing a microfilm cartridge. The custodian could not explain what had happened to the cartridge but surmised that the district returned it to the service center for destruction. Another custodian had 444 more cartridges than his records showed and was unable to explain the discrepancy.

The procedures followed at Dallas and other locations showed that custodians did not prepare the control records properly, perform the prescribed physical inventories, or reconcile inventory results to the records. These weaknesses may relate to the applicable guidelines not explaining the purpose for or the mechanics of how to perform these functions.

Package inspection program

IRS regulations issued in June 1976 require a package inspection program at service centers, the National Computer Center and the data center. The guidelines provide that the program be implemented by September 30, 1977.

The Ogden service center implemented a program prior to the new regulations. Center personnel inspected all briefcases carried by IRS employees and visitors entering or leaving the building.

CONCLUSIONS

Essential elements of IRS' security system include physical features, security guards, badge systems, and package inspection programs. Of the facilities visited, only Ogden had a package inspection program, but IRS is expanding this requirement to other facilities. Besides providing barriers to unauthorized access, these elements serve as visible evidence to the general public and Service personnel of IRS' intent to keep tax data confidential. We believe these elements adequately prevent general access.

There are, however, many weaknesses in the physical security program, most of which stem from lack of implementation and failure to monitor compliance. Consequences include little assurance that tax data shipments are received or that microfilm records on thousands of taxpayers are adequately protected. A possessor of a counterfeit badge or an authentic one belonging to someone else could enter a facility and the extent of his access within the facility would depend on the badge color. IRS also has recognized, and is willing to accept, the risk inherent in the present widescale exposure of tax data to guards, janitors, and technicians.

Collectively, the physical security weaknesses indicate either a lackadaisical attitude toward security or, at least, a downgrading of security measures in relation to other functions of the Service.

RECOMMENDATIONS TO THE COMMISSIONER OF INTERNAL REVENUE

To attain more protection from the physical security program, we recommend that the Commissioner of Internal Revenue:

--Revise procedures to require that badges clearly distinguish non-IRS personnel from IRS employees.

--Establish a requirement that badge records be compared on a test basis to the badge being worn by the holder of record and more adequately implement the present requirements to maintain accurate records and perform periodic reconciliations.

--Require, where volume permits, that tax data be adequately secured after normal duty hours in those areas where guards, janitors, and other non-IRS personnel have access, and that cleaning be performed in the presence of IRS employees to the maximum extent possible.

--Increase compliance monitoring activities by security managers.

--Revise guidelines to require management monitoring of tax data shipments through periodic reports showing unacknowledged shipments, days the acknowledgment has been overdue, and followup actions taken.

--Revise microfilm accountability and control guidelines to specify control record format and preparation instructions, physical inventory and reconciliation procedures, and procedures for reporting discrepancies to management.

IRS COMMENTS

IRS agreed with our recommendations and said that it has taken or plans to take corrective action. (See app. I, pp. 81 to 82.) Specifically, IRS said that it has designed and is testing a combination identification card and badge which will clearly distinguish non-IRS personnel from IRS employees. IRS projected that the new badge system will be implemented servicewide in fiscal year 1979. In the interim, IRS said it is changing its instructions to require that accuracy of the badge records be verified by tracing at least 25 percent of the recorded badges to the badge holder. IRS' Internal Audit will periodically ascertain whether the required verification is being accomplished.

IRS also said that it will issue new instructions requiring, where volume permits, that tax data be locked in security containers after normal duty hours in those areas where guards, janitors, and other non-IRS personnel have access. It will also (1) arrange to the maximum extent possible for cleaning to be performed in the presence of IRS employees, (2) formulate and implement a uniform receipt and management monitoring program for tax data shipments, and (3) establish standard operating procedures for microfilm accountability and control.

IRS plans to emphasize increased compliance monitoring activities by its security managers at all organizational levels. IRS said that national office security professionals will conduct annual, indepth, onsite reviews of field office compliance with security requirements.

Monitoring will also be conducted by responsible security managers at all major field installations and emphasis will be placed on security awareness and compliance as an evaluation factor in managerial performance reviews. IRS' Internal Audit will continue to perform independent tests to insure that security monitoring is being regularly conducted.

CHAPTER 8

CONTROLS TO SAFEGUARD TAX

DATA AT FEDERAL RECORDS CENTERS

Federal Records Centers store processed tax data, including tax returns. Considering that each IRS service center processes an average of 12 million tax returns annually, that individual returns are stored for a minimum of 6 years, and that corporate records are stored indefinitely, the need for Federal Records Centers' safeguards is readily apparent.

Certain weaknesses in the Federal Records Centers' security measures could result in unauthorized access to and disclosure of taxpayer data. However, because of the sheer volume of stored tax data and the filing system, it would be difficult to locate a specific tax return without first obt ning from IRS the location number for the desired document. Any unauthorized access would, therefore, probably be of a random nature as opposed to a premeditated effort to illegally obtain information on a specific taxpayer. Even so, any unauthorized disclosure would compromise the integrity of the Government's efforts to properly safeguard tax information.

PHYSICAL FEATURES TO RESTRICT ACCESS WERE ADEQUATE

The Kansas City service center uses the Kansas City Records Center and the Ogden service center uses the Denver Records Center. Both records centers, located on Federal reservations and enclosed with security fences, have either locked or guarded entrances. Denver receives added protection from steel doors, heavy steel mesh over all the windows, and a continuously monitored electronic intrusion system.

The Kansas City security system would not immediately detect forced entry into the center nor delay such an attempt long enough for the guard force to prevent actual penetration. Yet, considering the volume of stored data, the difficulty of obtaining specific returns, and the present level of security available, any substantial cost to increase the effectiveness of the center's security does not appear warranted.

ACCESSES BY RECORDS CENTER EMPLOYEES

The taxpayer should be assured of the confidentiality of his tax data whether it is in the hands of IRS or stored at a records center. Records center employees should have an official need to access tax returns from storage. Although no system will absolutely prevent an employee from randomly viewing tax returns to satisfy his curiosity, controls should be established to prevent easy access to a specific return for unauthorized reasons.

To control and locate returns, IRS assigns each a document locator number for service center processing. Certain subsequent actions, such as selection of a return for audit, necessitate assigning the return a new locator number. The records centers store returns according to the IRS assigned numbers.

To locate a specific taxpayer's return from storage, a records center employee would first need to obtain the current number from IRS. Because of the sheer volume of data and the complexity of the filing system, the task of finding a specific return without first obtaining the number would be almost impossible. Thus, barring collusion, it would be very difficult for a records center employee to improperly obtain a specific tax return.

PERSONS OTHER THAN RECORDS CENTER EMPLOYEES ALLOWED UNESCORTED ENTRY INTO AREAS CONTAINING TAX DATA

Records centers store tax data throughout the facility. Procedures permit storage area access by records center employees but deny access to all non-Government visitors. Center procedures permit Government visitors to enter the storage area only if accompanied by a records center employee.

Despite the policy, both records centers permitted janitors, guards, and General Services Administration maintenance personnel to enter the records storage area unescorted. The Kansas City center also allowed contract janitors in the storage area. In addition, management at both records centers provided keys or lock combinations to an unknown number of guards and maintenance personnel. Some of these personnel routinely entered the facility when no records center employees were present.

At our suggestion, the Denver Records Center changed the lock combination, thereby preventing maintenance personnel from entering the storage area without admittance by records center employees. A Kansas City official said he was in the process of working out an agreement with the General Services

Administration whereby only the building manager would have a key to the storage area. These actions should improve security.

At Denver, Air Force employees had worked unescorted in the storage area for over 15 years. These Air Force employees could have accessed tax data since the center stores Air Force and IRS records in the same area. IRS' Internal Audit previously pointed out this problem in September 1974. But nothing changed.

CONTROLS OVER REQUESTS FOR TAX DATA ARE ADEQUATE

Only IRS can request tax information from the records center and most requests are made on prescribed IRS forms. One copy of the request form accompanies the tax return sent to IRS, and one copy is placed in the file to provide a record showing what happened to the tax return and, in some cases, who requested the return.

Occasionally, IRS employees make telephone requests. The records centers accept these requests only if the requester's name appears on an IRS list of authorized persons. The centers furnish the requested information on a "call back" basis only to designated telephone numbers. The centers maintain a record of the telephone requests and file them with the tax returns.

In emergency situations, the records center will process a hand-carried request provided IRS gives prior notification. IRS must furnish the center with a list of persons authorized to deliver and pick up emergency requests or the IRS person obtaining the tax return must show proper IRS identification and sign for receipt.

IRS does not acknowledge receipt for mailed tax returns

No acknowledgment procedure exists for tax data shipments mailed from records centers to IRS. The centers return a copy of the IRS request with the data when shipped but procedures do not require the IRS recipient to acknowledge receipt. Therefore, except for negative responses, the centers have no assurance that the data was received and there is no system to provide timely notice of lost shipments.

CONCLUSION

Federal Records Center facilities and security measures were sufficient to deter accesses by the general public. While a penetrator could perhaps gain access without detection, it would not appear cost beneficial to increase the physical facets of the centers' security to maintain confidentiality of the documents stored therein.

Two factors, the filing system and the volume of stored tax returns, provide the greatest security for a specific tax return in a Federal Records Center. Unlike the situation within IRS, a penetrator, even given records center employment, would have great difficulty locating a specific return barring collusion with an IRS employee having access to locator information. The filing system, while incapable of preventing random accesses, makes access to a specific return very difficult.

Records center controls were sufficient to make certain that returns were provided only to IRS employees. But to increase control over the tax data, a receipt acknowledgment system should be established for tax returns mailed to IRS.

RECOMMENDATION TO THE COMMISSIONER OF INTERNAL REVENUE

We recommend that the Commissioner of Internal Revenue work with the Administrator of the General Services to establish a receipt acknowledgment system for tax data.

IRS COMMENTS

IRS said that it will work with the General Services Administration to establish a system for controlling tax data shipments and for providing timely notice in the event a shipment is lost.

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

Commissioner

MAY 31 1977

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

Dear Mr. Lowe:

We appreciate the opportunity to comment on your proposed draft report of April 21, 1977 entitled "IRS' Security Program: Improvements Are Required to Protect Tax Data Confidentiality." Your independent review of our security practices and the discussions between our staffs have been very helpful in identifying areas that require greater attention by our operating officials. I suspect that our long organizational history with a very low experience of actual losses or disclosures has contributed to a feeling among our management officials that security of tax data has not been a major problem. This feeling is being changed.

As the draft report notes, many of the comments and recommendations are similar to those contained in your January 1977 report on our proposed Tax Administration System (TAS), and consequently corrective action has already begun. Many of your findings had previously been identified by our own internal audit procedures, and corrective action was initiated prior to the issuance of the draft report. In addition, the control weakness that allowed a GAO auditor to generate a refund to himself had already been identified by the Service's internal audit staff, and corrective action was pending implementation. As you know, we share your view that TAS can provide a high level of protection, and feel that this new system will itself significantly improve our ability to control access to information requiring confidentiality.

We agree with the majority of the recommendations you have made, as is indicated in our response to specific items in the attachment to this letter. Although we have not been as aggressive as we might have been in the past in correcting situations that potentially weakened our overall security posture, I am committing the Service to a vigorous course of improvement. I am confident that this program will overcome the potential problems that have been identified.

Action to implement your recommendations has already begun, and will largely be completed before the next tax filing period. We have also started efforts to improve our own attitudes about the need for maximum security of tax information, and efforts to ensure compliance with existing security requirements.

- 2 -

Mr. Victor L. Lowe

To this end, we have:

-- devoted a considerable portion of our recent joint conference of Regional Commissioners, District and Service Center Directors to a discussion of means of obtaining compliance with security requirements and procedures;

-- initiated a security awareness program for all employees;

-- begun to more effectively use our existing evaluation programs to monitor compliance with security requirements;

-- initiated a major "risk analysis" effort to identify and prioritize the threats to our operations and the confidentiality of tax information;

-- approved in concept the creation, testing and evaluation of full-time district office Security Officer positions in one region;

-- confirmed your principal recommendation of centralizing security responsibilities, and are now determining the proper organizational location and plan for implementing such an office;

-- commenced development of a major training effort designed to instill sound security principles in all Service supervisors and managers.

I believe these initiatives, together with the implementation of most of your recommendations, will provide the highest reasonable level of security for tax information.

With kind regards,

Sincerely,

Commissioner

Attachment

GAO note: Page references in IRS' comments may not correspond to pages in the final report.

ATTACHMENT

Responses to GAO's Recommendations to the Commissioner

1. "Establish an independent office responsible for all facets of the security program at all IRS facilities. This office should be directly responsible to the Commissioner for developing procedures and controls to implement IRS' security policy. It should also be responsible for monitoring compliance at all IRS facilities and reporting all instances of non-compliance to local management and the Commissioner."

   The Service has previously indicated to the GAO 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."

   The Internal Revenue Service Security Council, which has overall policy responsibility for the formulation and implementation of the IRS security program, has initiated a study concerning all facets of the securi related to tax information. This study has been on-going since early February 1977. The study group's findings, thus far, confirm the GAO recommendation that the Service establish an independent security office, and the Service will take positive steps to move in that direction.

   Last month an in-depth review of the entire Internal Revenue Service organization was initiated. The precise organizational location and the plan for implementing the IRS security office will be determined by the organization review study team.

2. "Establish a procedure whereby programmers and analysts must obtain written authorization from the National Office before using actual tax data for testing."

   We agree with the concerns raised in the report and the need for tighter controls in this area.

   As a matter of policy, actual tax data will no longer be used for testing purposes unless specifically required - when a production type environment must be present or when it is too impractical to use any other data.

   We will establish procedures to limit the use of actual tax data for testing at the National Office Computer Facility. Programmers and analysts will be required to obtain approval from designated personnel at the National Office. However, in our field installations prior written National Office authorization may not be obtainable when tax data is required for testing. Therefore, in each Service Center and the National Computer Center the central control function responsibilities will include approval and control of the use of actual tax data for testing purposes.

3. "Establish a procedure for periodic review to determine that programs and program modifications are authorized."

   As we indicated in our response to the prior GAO report concerning Safeguarding Taxpayer Information - an Evaluation of the Proposed Computerized Tax Administration System, dated January 17, 1977 (LCD-76-115) we agree with this need. We are developing automated program modifications, authorization and control system with audit trails of updates, periodic matching and verification of consistency of field programs and software with the National Office masters. At each center the central control function responsibilities will include assurance that only authorized production programs and program modifications are authorized.

4. "Establish a check-out procedure for program documentation."

   We recognize the need to control program documentation. Therefore, all computer operations documentation has recently been reclassified and removed from the Freedom of Information reading rooms and has limited distribution to personnel. Also, very sensitive documentation, such as that which contains formulas for selecting returns for examination has very limited distribution and is carefully controlled.

   Additional controls will be implemented to require that only computer operators will be allowed to operate the computers, (recommendation number 5) thus restricting unauthorized computer use. Stricter control over programs and program modifications by the central control function in each center will be established as indicated in recommendation number 3.

   We will review our procedures, both at the National and field offices, to determine if sign-out or check-out procedures should be established.

5. "Establish guidelines to govern who may and may not operate the computers."

   We agree with the recommendation and will incorporate appropriate guidelines in our computer operations and management handbook instructions. These guidelines will be issued immediately.

6. "Require that computer personnel closely monitor equipment manufacturer engineer activity."

   We agree with this recommendation. We have current procedures which require this control. We will follow-up by contacting each center regarding this. Periodic checks will be performed during National and Regional Office review processes.

7. "Establish procedures whereby National Office Computer Facility job requests receive supervisory approval and tape librarians maintain records identifying the magnetic tapes used and who accessed them."

We agree with the first part of this recommendation. Division Directives on this have been unclear and inconsistent. These will be reviewed and revised where necessary to require supervisory approval for each job submitted. Management enforcement will be strongly emphasized.

We disagree with the second part of this recommendation based on the following: Approximately 1000 computer tests are run per day, each using several reels of tape. To maintain a record of each magnetic tape used and who accessed them would be prohibitively expensive and cumbersome. Since we are dealing in a test environment, the commitment of such resources would not seem worthwhile when compared to the degree of risk involved.

8. "Require that tape library access be restricted to library personnel and that tape charge-out records be properly prepared and maintained."

We agree that tape library access should be restricted but feel there are occasions when other than library personnel need access to the library. For instance, procedures require the IDRS System Security Administrator at the service centers to place in, and remove from a security cabinet, in the tape library, tapes identified as security tapes. Also, there may be occasions, especially on weekends, when there may be operating personnel on duty when no library personnel are there and access to the library is necessary due to unforeseen problems, reruns, errors, etc.

Current procedures restrict library access to library personnel, Computer Branch Chiefs, the IDRS System Security Administrator and those persons specifically approved by the Chief, Computer Branch.

We also agree that tape charge-out records must be properly prepared and maintained. Current procedures make it the responsibility of library personnel to document the removal of all tapes and disks from the library. Media which has not been returned within a reasonable or agreed time should be accounted for.

We will shortly follow-up with the field stressing the need for continuing management review and involvement to ensure compliance with published procedures.

9. "Revise inventory guidelines to require that all magnetic tapes and disks be periodically inventoried at all tape libraries; that inventory results be reconciled to the tape records; and that missing tapes and disks be accounted for.

We currently have handbook procedures which provide for the actions recommended pertaining to magnetic tapes. These procedures require an annual tape inventory as mandatory and highly recommend a semi-annual tape inventory. These procedures state that inventories are to be reconciled to the tape library records and all missing tapes are to be accounted for. Results of the inventory are to be sent to the National Office for review. We will implement procedures requiring semi-annual inventories.

All centers were instructed to conduct a disk inventory in April 1977 and have submitted this information to us. A requirement for semi-annual disk inventories will be established.

Follow-up will be performed through appropriate management action. We will also make this a part of our National and Regional Office review procedures.

10. "Establish a uniform procedure whereby authorized requestors sign for receipt of computer printed data.

We understand this recommendation to have reference to printed data from special requests, such as, for program testing or production problem solving, and not to printed data produced in normal production processing, for which we have an extensive transmittal process. With this understanding, we agree with the recommendation.

We will issue procedures within the next few months which will provide for a standard log to be maintained indicating the disposition of printed data and punched cards and for a receipt procedure system.

11. "Periodically assess whether security administrators submit employee profile changes for national office approval."

Presently the National Office specifies the profile to be used in particular areas within each organization. This does not allow field management the prerogative to define where work will be accomplished.

We realize there must be strict control over granting employees the right to use the different command codes. We are in the process of establishing procedures which will allow the field to develop and maintain the profiles in their offices with review by the National Office.

12. "Revise procedures to require that profiles of former operators be deleted within one work day after reassignment, furlough, or termination."

Our objective is to accomplish deletion of profiles of former operators within one work day after reassignment, furlough or termination and in most cases only one day is required. However, there may be some cases where this is not possible.

New procedures have been issued which require this deletion action be taken as soon as possible and no later than three days after reassignment, furlough (for a period of more than two weeks) or termination.

We will monitor this area by a closer follow-up by the system security administrators, by tighter managerial control and review by National and Regional review processes and visitations.

13. "Determine whether service centers have adequately implemented the June 1976 security tape control and accountability procedures."

We will contact each service center to determine the status of this item. Each service center will be asked specifically if they have provided the proper security cabinet, to identify which tapes and listings are given this added protection and what records are maintained showing who removed and returned security tapes and when. We will make this a part of our National and Regional Office review processes.

14. "Establish a procedure whereby the system security manual is distributed only to those having a need for it; a record is maintained of the individual recipients; and proper disposition is made of unneeded or obsolete manuals."

We agree with the above recommendation and realize the current method of distribution has not been working properly. We will take necessary corrective actions as soon as possible.

In addition, we will establish a procedure by October 1977 for maintaining a record of the individual recipients. We already have procedures for proper disposition of unneeded or obsolete manuals.

15. "Require that recipients properly safeguard the security manuals."

A distinctive cover sheet is being developed for attachment to certain sensitive documents stating the protection point value required and the type of protection to be provided. Requirements will also be established to make the recipients accountable for these documents at all times. Monitoring of these procedures to ensure compliance will be included in the criteria being developed for Recommendation No. 30.

16. "Develop and implement a retrieval system training module to preclude the use of actual tax data, while training system users. In the interim, establish procedures requiring reviewers to spot check training accesses to see if the operator had a legitimate need to access particular taxpayer accounts."

A computer assisted training module was implemented in January 1977. This modification directs the bulk of training needs for tax account information to fictitious data on a training file.

There remain a few functions in IDRS for which training does access production data on subsidiary files. These data do not have the disclosure ramifications that exist in tax account data. Because of the minimal need for training in these functions and/or the danger of systemic errors which could mix production and training data, they were not included as part of the training module. Alternatively, we are reviewing our planned changes for analysis of the audit trail file (covering terminal activity) to identify any unauthorized use of the system in these areas.

17. "Amend agreements with States to require that both the cognizant service center and district director be simultaneously provided the lists of State representatives authorized to request tax data and any subsequent changes to the list."

Omission of the requirement from the current IRS standard form (Agreement on Coordination of Tax Administration with State tax agencies) that lists of State tax agency representatives are to be furnished simultaneously to both the applicable service center director and the appropriate district director is an oversight which the Service will correct. This change will be incorporated in the next revision of the standard form agreement.

In the meantime, IRS will notify, by letter, each state tax agency with which the Service has an agreement that lists of designated State agency representatives are also to be sent to the service center which processes returns filed within the jurisdiction of the district office covered by the agreement.

As part of IRS' revision to this year's edition of Publication 664, Federal-State Exchange Program, which details to state tax agencies their data usage responsibilities as a participant in the IMF tape exchange program, the Service has specified that the list of designated state tax agency representatives is to be sent to both the district director and the appropriate service center director.

18. & 19. "Reemphasize the importance of limiting restricted area access to only those having an official need by requiring responsible officials to reevaluate and document the reasons why so many people have been granted access."

"Establish procedures requiring that districts restrict microfilm room access to only a few designated employees and that these employees fill only written requests."

A memorandum is being prepared to all field officials reemphasizing the importance of restricted area controls and the need to limit access to all such areas. We will also review all existing restricted areas to determine the need for continuing to limit access based on the criticality of the operations and review other critical operations not now so designated.

We have already recognized a weakness in our entry control procedures for restricted areas and have started a test at the Cincinnati Service Center and District Office to restrict access on computer-assisted basis rather than utilize employee monitors who are prone to human error. Current test findings are positive and further implementation at other locations seems promising. This new procedure will provide much tighter entry controls, a complete audit trail of all persons accessing the areas, and will definitely reduce the number of persons authorized to enter such areas. Instructions will also be issued to district office microfilm personnel to honor only written requests for data.

20. "Revise restricted area sign-in/sign-out register format to show the person to be contacted and the purpose for entry; and establish procedures for reviewing the registers to determine who entered the area and the need for entry."

Our register will be changed to include the additional information recommended and we will also issue instructions to require that security program personnel and managers responsible for restricted areas periodically review the register to determine who entered the area and the need for access.

21. "Revise guidelines to require that supervisors either review and approve requests for tax data or use a valid sampling plan to spot-check tax data in possession of employees to determine that only needed data is being obtained."

The Service is cognizant of the problem cited. Occasionally employees receive more tax information on a specific taxpayer than is actually needed. However, we recognize the need to re-emphasize the requirement for supervisory review and control of data requests in those areas where the requests are low in volume. In those areas where high volume of data requests prohibit a 100% review, we will re-evaluate existing guidelines, including consideration of sampling programs, to further assure that only required data is requested.

22. "Revise procedures to require that microfilm researchers fill requests for limited data by recording it on and then returning the request form rather than providing a complete transcript."

We agree with this recommendation to the extent that it relates to data such as that set forth in the example cited on page 51 of the draft (SSN or verification of name and address). Information such as this might be recorded on the request without significant resource impact. We will review our procedures and consider revising them to record such information on requests.

Adoption of this recommendation regarding the thousands of other requests for data received daily would unnecessarily burden a function that is essentially a simple, but extremely important high volume activity. Transcription of other than easily identifiable data would cost substantial staff hours and introduce human error in manual transcription.

23. "Consider alternatives for eliminating from microfilm transcripts all data not pertaining to the taxpayer that is the subject of the request."

A modification to the present viewer-printer equipment is now being tested, which would have the capability to mask out all of the extraneous accounts except for a limited amount of information from accounts immediately adjacent to the account being retrieved.

IRS has been conducting research to develop retrieval systems which would have the capability to completely eliminate all extraneous information. When the existing viewer-printer systems, which are now more than ten years old, are replaced, one of the mandatory features of the new system would be that only requested accounts would be furnished to users.

24. "Specify a three-day criteria for requesting all background investigations."

We had recognized this lack in existing procedures which specified a 3-day time limit for requesting NACI (National Agency Check and Written Inquiry) investigations but did not set a limit on requesting background investigations. A recently issued revision of investigation requirements provisions has corrected this problem by specifying that background investigations must be requested within one week of the employee's entrance on duty.

While the time limit we have set is one week rather than 3 days as GAO recommended, we think it fully meets the intent of the recommendation.

25. "Establish control systems for monitoring compliance in meeting the three-day and nine-month goals for requesting and completing background investigations. As a minimum, the control systems established should provide for periodic follow-up action, identification of instances where the goals are exceeded, and management reports explaining the reasons why the goals were not met."

We agree with the GAO recommendation that control systems should be established to monitor the timely initiation and completion of background investigations.

National Office control programs, including periodic field visitations, currently monitor compliance with the timeliness of requesting and completing background investigations. We are in the process of establishing additional control systems for more effective case control such as a management information system to provide periodic computer data on initiation and completion of background investigations, and a monthly case aging report from each regional office to monitor all overage cases. In addition, new procedures are being instituted in the employee audit program so that tax audits in connection with background investigations can be completed with the least practicable delay.

The Service currently has procedures whereby instances of non-compliance with established goals are referred to appropriate management officials for remedial action.

26. "Establish procedures requiring local management to ascertain the results of background investigations conducted by other agencies on non-government personnel who work in IRS facilities."

We will contact the Administrator of General Services to request that his regions be instructed to furnish IRS local management with the results of background investigations conducted by GSA on non-government personnel such as guards, cleaners, cafeteria personnel, etc. who work in IRS facilities. We will also include requirements for background checks in our own contracts and explore the feasibility of requiring building lessors to do the same in our leasing agreements. Also, we will request from GSA the delegated authority to award major contracts, such as guard and cleaning, to enable us to better control the activities of these non-government persons in IRS facilities. Should this delegation authority not be provided, we will then seek legislation to obtain this objective.

27. "Revise procedures to require that badges clearly distinguish non-IRS personnel from IRS employees."

A new ID card/badge has been designed and is presently being tested in Central Region. It clearly distinguishes all non-IRS personnel from IRS employees. It is contemplated that this new card/badge will be issued Servicewide in FY-79.

28. "Establish a requirement that badge records be compared on a test basis to the badge being worn by the holder of record and more adequately implement the present requirements to maintain accurate records and perform periodic reconciliations."

Our instructions are being changed to require that issuing officials at least annually verify the accuracy of both the numerical and alphabetical badge records by tracing at least 25% of the outstanding badges to the badge holder.

In addition, our Inspection Service will audit the badge records of each issuing official and ascertain whether required verification is being accomplished.

29. "Require, where volume permits, that tax data be adequately secured after normal duty hours in those areas where guards, janitors, and other non-IRS personnel have access, and that cleaning be performed in the presence of IRS employees to the maximum extent possible."

We will issue new instructions which will require, where volume permits, that tax data be locked in security containers after normal duty hours in those areas where guards, janitors, and other non-IRS personnel have access. In addition, we will see that cleaning of all Service space be performed in the presence of IRS employees to the maximum extent possible. This latter requirement can be met by day time cleaning to the extent that funding is available.

30. "Increase compliance monitoring activities by security managers."

We plan to correct past weaknesses by having the responsible security professionals in the National Office Protective Programs Branch carry out annual, indepth, on-site reviews of representative field offices' compliance with security requirements. In addition, monitoring will be conducted by responsible security managers at all major field locations with emphasis being placed on security awareness and compliance as an evaluation factor in top managerial performance reviews. The National Office will be evaluating in its scheduled National Office Review Program (NORP) how well the regional offices monitor compliance with security directives. Our Inspection Service will continue its independent testing and auditing to ensure that the security program monitoring is being conducted on a regular basis.

31. "Revise guidelines to require management monitoring of tax data shipments through periodic reports showing unacknowledged shipments, days the acknowledgement has been overdue and follow-up actions taken."

We will review our receipt guidelines concerning tax data shipments and proceed with formulation and implementation of a uniform receipt and management monitoring program.

32. "Revise microfilm accountability and control guidelines to specify control record format and preparation instructions, physical inventory and reconciliation procedures, and procedures for reporting discrepancies to management."

As recommended in your January report on the proposed Tax Administration System we are adding standard operating procedures for accountability and control of microfilm.

33. "Work with the Administrator of the General Services to establish a receipt acknowledgement system for tax data."

We will work with the General Services Administration toward establishing a system for controlling shipments of tax data which will provide a timely notice in the event a shipment is lost.

PRINCIPAL OFFICIALS RESPONSIBLE FOR ADMINISTERING ACTIVITIES DISCUSSED IN THIS REPORT

	Tenure of office	
	From	To
SECRETARY OF THE TREASURY:		
W. Michael Blumenthal	Jan. 1977	Present
William E. Simon	Apr. 1974	Jan. 1977
George P. Shultz	June 1972	Apr. 1974
John B. Connally	Feb. 1971	June 1972
COMMISSIONER OF INTERNAL REVENUE:		
Jerome Kurtz	May 1977	Present
William E. Williams (acting)	Feb. 1977	May 1977
Donald C. Alexander	May 1973	Feb. 1977
Raymond F. Harless (acting)	May 1973	May 1973
Johnnie M. Walters	Aug. 1971	Apr. 1973
ASSISTANT COMMISSIONER (ADMINISTRATION):		
Joseph T. Davis	Aug. 1974	Present
Joseph T. Davis (acting)	Feb. 1973	Aug. 1974
Alvin M. Kelly (acting)	Oct. 1971	Feb. 1973
Edward F. Preston	Sept. 1960	Oct. 1971
ASSISTANT COMMISSIONER (COMPLIANCE):		
Singleton B. Wolfe	Mar. 1975	Present
Harold A. McGuffin (acting)	Feb. 1975	Mar. 1975
John F. Hanlon	Jan. 1972	Jan. 1975
John F. Hanlon (acting)	Nov. 1971	Jan. 1972
ASSISTANT COMMISSIONER (ACCOUNTS, COLLECTION, AND TAXPAYER SERVICE) (note a):		
James I. Owens	May 1977	Present
James I. Owens (acting)	July 1976	May 1977
Robert H. Terry	Aug. 1973	July 1976
Dean J. Barron	July 1971	Aug. 1973

	Tenure of office	
	From	To
ASSISTANT COMMISSIONER (INSPECTION):		
Warren A. Bates	Jan. 1975	Present
Francis I. Geibel	Sept. 1972	Jan. 1975
Francis I. Geibel (acting)	May 1972	Sept. 1972
ASSISTANT COMMISSIONER (DATA SERVICES) (note a):		
Patrick J. Ruttle (acting)	Jan. 1977	Present
ASSISTANT COMMISSIONER (PLANNING AND RESEARCH):		
Anita F. Alpern	May 1975	Present
Anita F. Alpern (acting)	Jan. 1975	May 1975
Dean J. Barron	Aug. 1973	Dec. 1974
Lancelot W. Armstrong (acting)	July 1972	Aug. 1973

a/Effective January 2, 1977, responsibility for IRS system design, programming, and analysis as well as National Computer Center and Detroit data center operations was transferred from the Assistant Commissioner (Accounts, Collection, and Taxpayer Service) to the Assistant Commissioner (Data Services).