

DOCUMENT RESUME

03120 - [A2313455] (~~Restricted~~)

Released
10/13/77

[Review of Several Aspects of the Internal Revenue Service's Proposed Computerized Tax Administration System]. GGD-77-73; B-137762. August 18, 1977. 12 pp.

Report to Rep. John E. Moss; Rep. Charles Rose; by Elmer B. Staats, Comptroller General.

Issue Area: Tax Administration (2700).

Contact: General Government Div.

Budget Function: Miscellaneous: Automatic Data Processing (1001); Miscellaneous: Financial Management and Information Systems (1002).

Organization Concerned: Internal Revenue Service.

Congressional Relevance: Rep. John E. Moss; Rep. Charles Rose.

Authority: Privacy Act of 1974 (P.L. 93-579). Social Security Act, as amended; Internal Revenue Code 6103(a) (1). Tax Reform Act of 1976. P.L. 94-202.

Concern was expressed about the Internal Revenue Service's (IRS') Tax Administration System's privacy safeguards over the exchange and use of tax information, information and data management features, potential for and controls over linking with other Government and private computer systems. IRS' management structure's ability to support the system's advanced technology was also questioned. Findings/Conclusions: No plans were found which would violate current laws protecting the privacy of tax return information, and no covert, illegal attempts to link the system with any other computer system could be detected. Direct electronic linkage between the IRS' system and any other computer system should be decreed illegal and the transfer of data by any means between the IRS system and other systems should be allowed only when specifically authorized by law. IRS has planned for special coding access to terminals through use of passwords, system monitoring, no terminal to terminal communication capability, and audit trails as means of preserving security. Data input under the proposed system will be the same as in the current system, and the internal control features will probably not change. IRS has no plans to link the proposed system with any other system (Government or private) unless required by law to do so. If IRS implements its planned privacy and security controls, taxpayer privacy should be protected in accordance with established legislation. (SS)



~~RESTRICTED~~ Not to be released outside the General Account COMPTROLLER GENERAL OF THE UNITED STATES by the Office of Congressional Relations

24/55

B-137762

AUG 18 1977

Released 10/13/77

The Honorable John E. Moss and
The Honorable Charles Rose
House of Representatives

03120

Your joint letter of March 11, 1977, expanding on concerns raised in your June 8, 1976, letter, requested that we review several aspects of the Internal Revenue Service's (IRS') proposed computerized Tax Administration System. In summary, you expressed concern about the system's (1) privacy safeguards over the exchange and use of tax information, (2) information and data management features, and (3) potential for and controls over linking with other Government and private computer systems. You also requested that we assess IRS' management structure to determine whether it could support the Tax Administration System's advanced technology.

As you know, we have already completed one review of the proposed system, and have extensive work on the system currently underway. As agreed with your offices, we deferred work relating to your specific concerns until IRS could act on the recommendations contained in our January 17, 1977, report to the Congress, "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115). Deferral also allowed us to complete our review of IRS' current security operations; we believe IRS' actions to implement recommendations contained in that report ("IRS' Security Program Requires Improvements To Protect Confidentiality of Income Tax Information," July 11, 1977 (GGD-77-44)) would directly affect how much IRS could improve security under the proposed Tax Administration System. A copy of the report was previously sent to you.

Our January and July reports deal with overall security in both the present and proposed IRS systems; this report addresses your specific concerns.

We found that IRS has no plans which would violate the current laws protecting the privacy of tax return information of taxpayers. Moreover, we believe any covert, illegal attempt to link the computerized Tax Administration System with another computer system or any other illegal use of the system could be detected, given the environment in which it is being developed. We want to stress, however, that we found no evidence indicating that IRS will attempt or has

contemplated computer links that would be in violation of the appropriate Internal Revenue Code provisions and other statutes. We believe that the proposed system's security features and IRS' commitment to implement the recommendations contained in our July report will afford taxpayers a system that adequately protects the privacy of their tax returns.

SAFEGUARDS OVER THE PRIVACY OF INFORMATION

Concerns raised

You expressed these specific concerns:

- How are the legal mandates of IRS and the Social Security Administration to be fulfilled without violating the Privacy Act and GAO's proposal for prevention of exchange of data in such a manner?
- How can the two agencies carry out such a task without endangering the data and privacy of millions of citizens, especially given the state of the art and impossibility of safeguarding such information?
- How does the proposed Tax Administration System relate to the proposals of the National Commission on Electronic Fund Transfers and Office of Technology Assessment?
- What are the information privacy safeguards in addition to the physical security aspect?

Findings

You advised us of IRS' alleged plans to establish an electronic hookup with banks around the country for the purpose of checking on taxpayers' daily bank balances. You also pointed out that, to implement Public Law 94-202, Section 8, IRS would electronically share tax information for its planned information document matching program with the Social Security Administration. Such electronic transfer, you stated, would endanger the privacy of millions of citizens and might conflict with recommendations of the National Commission on Electronic Fund Transfers and the Office of Technology Assessment.

We found that IRS has no plans for bank hookups to check on taxpayers' daily bank balances. To do this would be both costly and without apparent statutory basis. As of March 31, 1977, there were about 15,200 banks nationally, excluding savings and loan institutions, and the cost to hook up with them would be extremely high. In addition, any IRS attempt to use such a hookup for transferring funds electronically or otherwise without the taxpayer's consent (except in cases such as duly processed attachment and jeopardy assessment) would be illegal. Both IRS and the consenting bank would be subject to any penalties established by the Congress and/or the State for any unauthorized or improper removal of funds.

The Tax Reform Act of 1976 generally requires IRS to notify taxpayers of summonses of their bank account records and allows them to contest summonses.

The National Commission on Electronic Fund Transfers, in its interim report dated February 23, 1977, would go a step further. The Commission recommended Federal legislation:

- Granting the individual the right to contest any Government access to his financial transaction information and providing for prior notification to the individual of any subpoena or summons. The legislation would take into account the legitimate needs of law enforcement and other Government agencies. Access by Government without due process as specified should be declared unlawful.
- Providing that all third-party private-sector use of information about a consumer's depository account without the specific consent of the individual be declared unlawful, except for information necessary to verify or complete transactions, to verify the existence of the consumer's account, or to give information regarding the improper use of the account.

As you know, the Privacy Act of 1974 (Public Law 93-579) generally prohibits sharing any information in Government files about individuals without their consent. However, Public Law 94-202 provides a statutory basis for IRS to exchange tax information with Social Security under the Information Document Matching Program. The exchange will not be electronic, but the law does not preclude electronic exchange.

Prior to the passage of Public Law 94-202, Social Security received data from IRS under the general provisions of Internal Revenue Code section 3103(a)(1) for administering title II of the Social Security Act, as amended. The data was used to credit an employee with social security quarters earned and applicable wages received. Under Public Law 94-202, Social Security will convert all employer wage and earnings statements (W-2s, W-2 Ps, and non-FICA W-2s) to magnetic tape for both its and IRS' use. After converting, Social Security will ship to IRS magnetic tapes containing data needed to match the wages claimed on taxpayers' returns to employer information returns. These tapes will be sent to IRS under current shipping procedures.

IRS has not considered the electronic transfer of such data, nor do we believe this method of transmitting such volumes of information is necessary. Four Social Security regional offices will be shipping data from about 184 million documents.

If each regional office used the fastest readily available wire transmission equipment and operated it 24 hours a day, complete electronic transmission of the data to IRS would take over two months. In addition, IRS does not need the data until 10 months after the close of the tax year. This should allow ample time for Social Security to prepare and ship the magnetic tapes.

Notwithstanding that IRS plans no electronic hookups to banks and Social Security, you raise an important future issue on the need to reconcile proposed electronic hookups to (1) the Privacy Act of 1974; (2) the proposals of the National Commission on Electronic Fund Transfers; (3) the privacy, due process, and security concerns of the Office of Technology Assessment; and (4) the recommendations in our January report. The concepts of electronic transfer of funds and electronic access to accounts are far-reaching. The lack of paper documents and the speed of electronic transfers have implications for consumers, banks, and the Government. We agree with the Office of Technology Assessment and the National Commission on Electronic Fund Transfers that electronic fund transfers are sufficiently different from conventional fund transfer methods to warrant special congressional consideration to conduct effective oversight and to develop a proper legal framework.

In our January report, we stated that the Congress may wish to consider legislation (1) making direct electronic

linkage between IRS' Tax Administration System and any other computer system unlawful and (2) allowing the transfer of data by any means between the IRS system and other systems only when specifically authorized by law.

Additionally, our January report discussed several of the proposed system's planned security features, including technical, administrative, and organizational controls as well as physical protection of the computer facilities.

The proposed system's safeguards include the use of a unique operator password for terminal access to the system. IRS is exploring computer-generated assignment and distribution of these passwords as a further protective measure. Operators will be required to insert a specially encoded identification badge for terminal activation, and this badge will be needed to gain access to the building and move about within the center.

Terminal and employee profiles will continue to be used. Each terminal will have a computerized profile restricting the actions which may be taken on that terminal. Likewise, employee profiles will prescribe those files to which each employee may have access and those actions the employee may process in the files. Allowable actions permitted an employee will be based solely on his assigned tasks. Unsuccessful attempts to enter the system will be monitored, and after three access tries, the terminal will lock, requiring supervisory intervention.

Under this system, a Security Administrator will be responsible for directing and coordinating security matters in each service center area. The Administrator will monitor the system's on-line activity and be alerted when terminal entry requirements are violated.

As in the present system, terminal-to-terminal communication will not be possible. Under the proposed system's design, field terminals will only be able to communicate with their host service center. Interservice center activity will be controlled by the National Communications Center, which will transmit data tape-to-tape over dedicated data channels.

Audit trails are another means of protecting the system. IRS plans to have comprehensive audit trails to show the record before and after the transactions and identify the person initiating the addition, deletion, or update, as well as the reason for the action. In this way, reconstruction

of any transaction or tax account record should be possible. Extensive audit trail and accounting records of intercenter activity will be maintained by the National Communications Center.

There will also be a network of administrative safeguards: prospective employee background checks, programs to develop employee awareness of security requirements, clearances for departing employees, supervisory review controls, and independent operational reviews.

Physical protection of IRS' data processing facilities will be continued by perimeter fencing, a security guard system, an electronic intrusion detection system, security lighting, and an employee identification system.

Movement within each center will be controlled, and access to the computer room and file library will be given only to employees with direct operational responsibilities. File and media use will be tightly controlled by comprehensive procedures for shipping and disposing of documents, magnetic tape library maintenance, quality review, equipment operation and maintenance, systems design, and program development.

Conclusions

System security depends on interaction of the numerous controls generally described here. These physical safeguards, organizational and procedural controls, programed measures, and hardware devices are interlocking, forming a network to protect the IRS data processing system from unauthorized access or abuse.

IRS improvements as a result of our January report and its commitment to implement the recommendations of our July report should result in a more secure Tax Administration System because many facets of IRS' current system will be carried forward into the new system.

IRS' proposed plans to exchange information with Social Security are in accordance with the enabling legislation. IRS' proposed security measures, if properly implemented, should result in a reasonable level of security.

INFORMATION AND DATA MANAGEMENT FEATURES

Concerns raised

Your concerns were these:

- How will the proposed system manage data input, storage, and handling?
- What are the internal controls over media (tapes, disks, etc.) and software documentation and data elements (how data is broken down and aggregated)?

Findings

IRS currently converts tax returns and related information to machine-readable form by transcribing it to magnetic tape using the Direct Data Entry System. Other types of data needed to carry out its responsibilities are received in either paper or magnetic tape format. IRS has no plans to modify this process under the proposed system.

In approving IRS' accounting system in June 1974, we pointed out that the procedures for internal control over the Direct Data Entry System were adequate. Although we have not made any extensive reviews of the implementation of internal control, IRS' internal auditors have spot-checked the system and found no internal control breakdowns in the Direct Data Entry System.

Under the proposed Tax Administration System, data will be stored both on magnetic tapes and in immediate access storage. This is similar to the current system in which the master files are stored on tape and the Integrated Data Retrieval System files are stored on disks. Software documentation--written descriptions of computer programs--will probably be controlled as is done in the present system. Both our January and July reports addressed the internal controls over data stored on tapes and disks, and software documentation.

The proposed system will affect the means of storing data. Data will be stored in computer-readable media for 5 years, rather than the 3 years as prescribed under the current system. IRS believes that storing data for an additional 2 years under the proposed system will allow automatic data processing technology to provide strict control over record accesses. Under the current system, the use of microfilm and other hard copy is subject to personal authorizations, the maintenance of logs, etc. Thus, IRS believes that the proposed Tax Administration System can make a major contribution to improving controls for privacy protection.

Data handling or data processing under the proposed system will be different from the current system. For example, much of the data now on tape will be in immediate access storage, such as disk storage; input error correction will be done on a real-time basis; input results from casework will be posted on a real-time basis; and mass input (tax return data) will be posted overnight on a batch basis. We could not evaluate the proposed system's data handling system because the system is still in a preliminary stage of development.

Your final concern in this area was how the proposed system's data elements will be broken down and aggregated. As you know, a data element is the smallest recognizable piece of data--a social security number, for example--and would not normally be broken down further. As to the aggregation of data elements, the main distinction between the proposed and current systems is that under the proposed system all the data elements pertaining to a particular tax entity would be available for recall without the need to search through various files for them. For example, the proposed system will be able to aggregate the status of cases, the relationships between different tax returns, and the results of prior years' audits.

In its current state of design, the proposed Tax Administration System will use 59 files--collections of related records--including backups, of which 28 will be on magnetic tape and 31 will be in immediate access storage.

Conclusions

The data input under the proposed system will be the same as in the current system. Data will be stored on magnetic tape and in immediate access storage. The internal control features over media (tapes and disks) and software documentation probably will not change under the new system.

IRS controls over media and software documentation were evaluated in both our January and July reports. IRS improvements as a result of our recommendations should improve its management of these.

POTENTIAL COMPUTER LINKAGES

Concerns raised

These concerns were expressed:

--What is the potential for linkage with other automatic data processing systems in or out of Government?

--What administrative and physical guarantees are there against such linkages?

Findings

As a result of reviewing the proposed Tax Administration System documents, and after discussions with IRS officials, we found that IRS has no plans or intentions to link the system with other systems in or out of Government. From a purely technical viewpoint, however, it would be possible to do so.

Many things would have to be done to accomplish such a linkage. IRS and the participating agency would have to make a conscious decision to break the law, money would be needed, and there would have to be a massive conspiracy both within IRS and the linking agency. Physical evidence of such linkage would also have to be created. If all of these things were done, technical problems could still inhibit the linkage. In addition, there would have to be a breakdown in the activities of agencies charged with oversight of IRS activities.

Linkage of computer systems involves the movement and use of data. The Privacy Act of 1974 and the Tax Reform Act of 1976 prescribe conditions under which agencies may move and use data. For example, the Privacy Act requires agencies to annually publish descriptive information on their record systems in the Federal Register and prohibits them from disclosing records for other than prescribed uses without prior written consent. Further, agencies' officials are subject to civil and criminal penalties for violations of the act. The Tax Reform Act of 1976 comprehensively treats the subject of who may use tax data under what conditions. Penalties and civil damages for misuse of data were further prescribed in this legislation.

A great deal of money would have to be obtained and a massive conspiracy would be required to install the necessary interface equipment and design, write, and operate the necessary computer programs. The organizations responsible for the systems design, programming, testing, operations, accounting, and internal audit are independent of each other. Further, the required equipment and data communication lines would be tangible evidence of linkage--evidence which in our opinion could not be disputed.

Certain technical problems could also make successful linkage difficult. For example, it would be impossible to get instant access to another computer's records if the records were on magnetic tape.

Also, the oversight activities of several external organizations would have to break down. GAO, the Joint Committee on Taxation, the Oversight Subcommittee of the House Committee on Ways and Means, and the House and Senate Appropriations Committees oversee IRS. Other organizations are also concerned with privacy issues, among them the Office of Technology Assessment, the Privacy Protection Study Commission, and the National Commission on Electronic Fund Transfers.

Conclusions

IRS has no plans to link the proposed Tax Administration System with the systems of any other Government agencies, organizations, or persons, unless it is required to do so by law.

We believe that the combination of current legislation on the use of tax data, the internal IRS organizational checks and balances, and the oversight activities of external organizations should expose any attempts in the planning stage by IRS to covertly link the proposed system with other computer systems. Further, we believe that our legislative proposals (see p. 4) would further tighten the restrictions on linking IRS computers to other automatic data processing systems.

ADEQUACY OF IRS MANAGEMENT STRUCTURE

Concern raised

This concern was expressed:

--Can the IRS management structure support this advanced technology, in light of the difficulty with the systems they now operate?

Findings

This question suggests concern over IRS' ability to control systems such as the Information Gathering and Retrieval System, which was discontinued in June 1975. Data misuse under this system raised concern as to whether IRS' management would permit misuse of the proposed Tax Administration System and whether IRS' management structure is such that misuse could continue undetected.

It is difficult to assess an agency's ability to control advanced technology before its implementation. However, as

discussed above, the basic mechanisms for internal oversight of the proposed system, as well as the present automatic data processing system, are in place. IRS' management has a role in the oversight process at the local, regional, and national office levels. Its internal audit function has responsibility for conducting a review program, including systematic verification, analysis, and appraisal of security measures. A branch of this division is devoted to data processing activities. A wide variety of methods (e.g., audit trails, facility controls, data controls, records of equipment operations) are available to oversee automatic data processing operations, and information on safeguard effectiveness is planned for continual review by IRS officials.

Each of IRS' organizational levels and the Internal Audit Division were involved in developing the plans for the proposed system, and their oversight responsibilities under the system would be a continuation of the functions currently performed. The Treasury Department provides additional oversight through its Office of Computer Science.

Additionally, in our January report on the system, we recommended that IRS establish a national data processing security office responsible for technical, administrative, and physical security to include all data processing facilities. Such an office should be independent of those organizational elements responsible for the development and operation of the computer systems and facilities and have authority sufficient to assure appropriate security.

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

IRS recognizes the merits of our recommendation, and as a result of our July report it will be expanding the responsibilities of this office to include all facets of security, not only automatic data processing operations. IRS is currently studying the concept to determine the proper organizational location for the expanded office.

Conclusion

If IRS implements the recommendations contained in our January and July reports, its internal organizational

structure should be strengthened to prevent misusing the proposed Tax Administration System.

Further, as discussed in the preceding section, we believe that the system is being developed in an environment much more attuned to privacy safeguards than was the Information Gathering and Retrieval System. Both the internal and external oversight functions afford controls for preventing misuse of the proposed Tax Administration System.

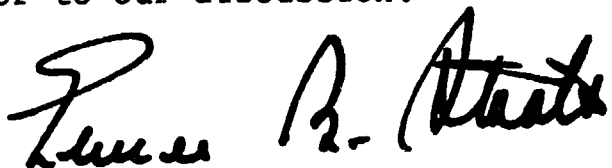
- - - -

In summary, we believe that if IRS implements its planned privacy and security controls and takes action on our recommendations, taxpayer privacy should be protected in accordance with established legislation. We believe that the internal and external organizational and oversight functions should expose any improper attempts to link the proposed system to other computer systems.

The House Subcommittee on Oversight, Committee on Ways and Means, and the Joint Committee on Taxation, in letters dated March 28 and May 31, 1977, respectively, requested us to evaluate the need for the system, system alternatives, the revised system cost/benefit analysis, the extent to which current privacy legislation and IRS' internal policies will protect taxpayers' privacy and security under the system, and the possible linkage of taxpayer accounts within and without IRS. This work should further insure that IRS' future use of computers is consistent with appropriate privacy and security requirements. When our work is done, you will receive a copy of our report.

We did not obtain IRS' formal comments on this report but, during the course of our review, we informally discussed our findings with them. Based on these discussions as well as our review of official IRS statements, testimony, and responses to our previous reports concerning the proposed Tax Administration System, we believe we have fairly taken into account IRS' views on the subject issues.

We will be in contact with your offices shortly to discuss the subsequent distribution of this report unless you publicly release it prior to our discussion.



Comptroller General
of the United States