4.6 SECURITY

ISSUE: WHAT ADDITIONAL SAFEGUARDS MIGHT BE NEEDED TO GUARANTEE THE PHYSICAL AND TECHNICAL SECURITY OF THE SYSTEM?

SUMMARY

Any computerized information system must be made secure against theft of the information, against accidents, sabotage and the like. The Internal Revenue Service has described a number of administrative steps and computer and systems restrictions addressed to such problems. While they go far toward meeting the system's needs, additional measures might be suggested for consideration as a means to a more effective job.

Furthermore, the description provided of TAS raises questions whether or not, once policy has been made for collecting, use, and managing the information, the system contains reasonable guarantees that it does not do what it is not supposed to do.

BACKGROUND

Public documents and Congressional testimony on TAS on the matter of security arrangements for TAS are vague, technical, and brief. They frequently blur the difference between existing safeguards and what is planned for TAS.

The TAS proposal filed under the privacy Act identifies existing programs in pre-employment screening, employee compliance, on-the-job education of employees to make them aware of their responsibilities, and management controls and reviews. It states that the Service intends to continue and strengthen these requirements as a part of the implementation of the proposed redesigned system. It has limitations on terminaI access through terminal profiles which define the functions and restricts the use of a terminal; an, employee profile, and internal file which contains the function each authorized employee can perform, the identification of the specific files, accounts, sections, and access codes which each employee needs to perform official duties; the identification badge, the physical identification of a system user; the employee password; and access codes.

It has audit trails recording how the system is used and by whom; at a minimum, according to the report, the employee identification, time, date, terminal of input, and access code are retained and spot-checked.

It has restricted accounts and files which means certain data is considered especially sensitive and is given extra protection. This restricts access to a specific account, to a specific section of an account, or to an entire file. In addition to security measures to be met for file access, an audit trail of successful and unsuccessful accesses will be maintained and followed up.

It has computer data checks, validity checks which verify the accuracy of the data, or systematic checks which test for postability to the data base. There is a computerized inventory of tax return charge-outs. There are data and accounting controls.

Inter-Service Center activity is controlled by channeling all activity requiring data from other than the originating center through the National Communications Center. An audit trail will be maintained of all inter-service center activity. When accounts are moved between centers, additional accounting records will be maintained at the National Communications Center. The National Center will maintain a central directory of all accounts for all service centers. All data movement between the NCC and a service center will be from tape-to-tape over dedicated lines.

There is a centralized system design in the National Office under the direction of one high level manager. Computer programming, procedures, writing, and equipment procurements is under this central direction. System analysts and computer programmers are not permitted to perform any production operations. This approach, it is stated, "provides additional protection against unauthorized systems changes and assurance of uniform programs and security checks and controls!"

The TAS proposal describes briefly plans for data communications safeguards:

> "To minimize the risk of unauthorized access to tax information through the data communications subsystem, the Service will have management and operational control of all devices which: process or are capable of processing tax information; account for the transmission of tax information; or control the transmission of tax information. All data will be communicated over dedicated transmission channels. Field terminals can only communicate with their host service center. Terminal to terminal communication cannot take place. Service center-to-service center communications must take place through the National Communications Center transmitting data from tape-to-tape in concentrated batches over encrypted lines. "

A number of physical safeguards are spelled out briefly.

The General Accounting Office has identified a number of problem areas in these security arrangements as they apply to the present Integrated Data Retrieval System. The Office also has

found no evidence of a present threat that would warrant cost of procuring encryption devices. It found that through proper design and implementation, TAS will be capable of providing high-level protection for taxpayer information. It reported, however, that some technical, administrative and physical safeguards *now used in* ADP *processing had some weaknesses and needed correction* within existing security procedures, methods, and controls.[29]

The IRS has indicated that they are addressing some of these problems.

Opinion on the panel was that the GAO had raised enough problems and revealed enough violations in the present system to suggest that some clear evidence from IRS of dealing with those problems in the new system would help those in Congress concerned about computer safeguards of the system.

while it was, of course, not the function of the panel to assess those security features planned for the new system, a number of problem areas in need of possible clarification because of the brief and general descriptions prodded, were pointed out by individtual members during discussions and these will be provided separately for the assistance of the Committee.

TO provide a factual basis for the Committee, these and other problem areas might be identified more fully with the assistance of the National Bureau of Standards Institute for Computer Sciences, the General Accounting Office, and other knowledgeable people in the computer industxy.

In addition to these security concerns which are standard for such a computerized information system, there is another aspect of the security Problem which is too frequently overlooked and TAS might be reviewed for this element of security. That is once policy decisions have been made for the collection, use and management of the information, once it has been determined by policy-makers in Congress and the Executive Branch what it is that they do and do not want done with the technology, how can it be determined that the system does not do what it is not supposed to do. While this question is an implicit one throughout the report, it bears further consideration in this phase of the consideration of TAS.

---

29. Report to the Congress by the Comptroller General of the United States. "Safeguarding Taxpayer Information — An Evaluation of the Proposed Computerized Tax Administration System." (January 1977).