

APPENDIX 2

IRS SUMMARY OF MAJOR TAS FEATURES – PRESENT AND PROPOSED SECURITY AND PRIVACY SAFEGUARDS

Present System

Proposed Tax Administration System

Physical Plant and Equipment Security

All computer facilities have complete electronic intrusion detection, silent trouble alarms, and related protection systems monitored at a protection console. Guard services, security lighting, and security fences are other physical safeguards.

Color coded photo badges, guards and receptionists are used to control entry to the centers and to restrict the movement of personnel and visitors within an installation.

Specific employees designated at each IRS office where terminals are located are responsible for security matters. Systems Security Administrator located in each center directs and coordinates security matters for the area.

“Pairing” Plan provides back-up location for each center in the event of loss of center’s computer or entire installation. NCC is backed up by a “sister” government agency.

Copies of master files are maintained in special disaster-proof facilities.

Personnel Integrity and Quality Assistance

Pre-employment screening of applicants, personnel investigations and clearances, investigations of complaints of misconduct or irregularities, and *development of employees’* awareness of standards of conduct and security *measures* are features of the IRS integrity program.

Will continue.

Will be replaced by magnetic stripe, photo badges which will be used in all offices with terminals or computer equipment. The new badge will be used to activate terminals, record the identifications of terminal users, and restrict access to data. Their use to control entry to the facility as well as to limit access to authorized areas within the facility via electronically controlled gates and automatic recordation of entries and departures is under study.

Will continue. Dual purpose badges described above will strengthen security measures in all offices.

Revised Plan has been outlined for decentralized TAS proposal. “Sister” agency back-up will be eliminated. NC will be paired with a SC.

Will continue.

Will continue.

Present System

Proposed Tax Administration System

Personnel Integrity and Quality Assurance (continued)

Supervisory reviews and approvals are required. Manual quality and output reviews are made with limited computer support.

Independent review and appraisal of operations are made by the Internal Audit Division.

Security Administrator is alerted when terminal entry requirements are violated.

System design, computer programming, software modifications, procedures writing, and equipment procurements are under central direction in the National Office. This approach provides additional protection against unauthorized systems changes, and assurances of uniform programs, security checks, and controls. For example, systems or computer program changes cannot be made through terminal input.

Identification data, passwords (periodically changed) command codes, terminal, account and other restrictions limit employees' access to "potentially active account" data available through IDRS terminals (approximately 10% of the accounts).

Title 26 U.S. Code 7213 provides fine or/and imprisonment and also dismissal from employment of Federal employees who unlawfully divulge tax information. (Fine and imprisonment also apply to state employees who receive tax information.)

Limited disclosure to public, congressional committees, states and other government agencies required by statutes, regulations and executive orders.

Computers will be used to the maximum extent practicable for early detection and correction of errors. Case terminal input operations will be monitored and checked for accuracy and acceptability during processing and prior to output printing. The scope of review will generally be based on a computer subsidiary file containing a profile of the employees' experience, training, and proficiency.

Improved computer assisted auditing techniques will provide greater coverage. Also on-line monitoring of terminal activity by Internal Audit Division (and Security Administrator) will assure better security.

In addition, Security Administrator will have new capability to monitor terminal activity.

Will continue.

Additional employee and terminal security computer files will be provided to insure access to only the specific files and data needed to perform official duties. The new magnetic stripe photo badges, previously described, will also restrict entry to terminals and access to data.

Will continue.

The Service has drafted legislative changes to provide additional restrictions. TAS will accommodate such changes.

Present System

Proposed Tax Administration System

Personnel Integrity and Quality Assurance (continued)

Detailed procedures issued on disclosures for Freedom of Information and other requests. The Disclosure Staff in the Office of Assistant Commissioner (Compliance) and Chief Counsel's Disclosure Division review requests and give advice on disclosure matters. Additional procedures are being drafted for the Privacy Act of 1974.

Additional procedures will be issued as necessary.

Data Controls

Centralized Master File from which manually prepared approved requests produce computer print-out transcripts. Computerized recordation of requests are not made. Manual controls exist mainly for follow-up purposes.

Microfilm data of a service center's accounts are available through manually prepared and approved requests and manual research. Accesses are not permanently recorded.

Approximately 10% of the tax account data is accessible to authorized personnel via IDRS terminals which have computerized restrictions, controls and temporarily retained audit trails.

Requests for tax return paper documents are manually prepared, approved and transmitted to the Federal Records Center or the service center. A copy of the request serves as a charge-out and replaces the return in the block folder. The new Audit Information Management System (AIMS) and its predecessor (SCRIP) are semi-computerized methods of locating tax returns in the Audit Division.

Most of the revenue accounting system controls are automated. However, some journals, reports and the general ledger are manual operations. (The accounting system has been approved by the Comptroller General.)

Numerous validity, error, and postability checks are made of every element of data which enters the system. Computerized data controls insure against loss of data between runs, programs, etc.

Decentralized Master Files will be accessible by terminal operators who will input approved requests. There will be computerized restrictions, controls and audit trails. Transfers of data between SCS will be controlled by NCC.

Microfilm operations will be eliminated (except for pre-TAS and old inactive accounts). Access to data by authorized personnel will be via terminal operation with computerized restrictions, control and audit trails.

Practically all accesses to master file data (five years) will be via terminals which have additional computerized restrictions controls and indefinitely retained audit trails.

All approved tax return requests will be input through terminals, thereby enabling the system to maintain a current computerized inventory and control of all requests, a permanent record of charge-outs, and periodic reports of outstanding returns. The AIMS will be integrated into TAS when it becomes operational.

The accounting system will be completely automated under computer control, including computer generation of journals, reports and ledgers.

Will continue.

Present System

Proposed Tax Administration System

Data Controls (continued)

Extensive library controls, trained production schedulers and proper job and personal identification of employees prevent unauthorized access to work files and programs.

Will continue.