29008

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

GENERAL GOVERNMENT
DIVISION

JUN 11 1984

B-215208

Mr. Arnold B. Gordon, Acting Director
Disclosure and Security Division
Internal Revenue Service

Dear Mr. Gordon:

Subject: Tax Information Safeguard Activity Annual Report (GAO/GGD-84-83)

This letter constitutes our annual report on safeguarding tax returns and return information. As agreed with the Former Director, Mr. Raymond L. Rizzo, this report covers the 2-year period from January 1, 1982, through December 31, 1983.

The annual report is required by Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines. That publication requires agencies authorized access to federal tax returns and return information to report (1) significant changes in safeguard procedures or authorized access to tax return information adopted over the period and any changes or enhancements to physical and computer security measures utilized to safeguard tax data; (2) the results of internal inspections conducted to assure that written procedures are followed together with identification of the offices visited, security tests performed, findings made, and overall safeguard awareness found; and (3) the identity of return information disposed of during the period and the date and manner of destruction. The following sections summarize our safeguard efforts in connection with each of these three reporting requirements.

CHANGES TO SAFEGUARD PROCEDURES

As you know, our safeguard policies and procedures are set forth in GAO Order 0135.1. This order, supplemented by your Publication 1075, establishes the necessary comprehensive framework for GAO employees to exercise control over tax returns and return information and thereby protect taxpayer information from unauthorized disclosure.

(268185)

029689
124566

Our interest, like yours, is to safeguard taxpayers' privacy rights by establishing the best procedures practicable. This means adjusting our procedures to account for any statutory or operational changes which affect the handling and control of tax returns or return information. Accordingly, we have been reviewing our written procedures in light of changes to our access authority included in the Tax Equity and Fiscal Responsibility Act of 1982. In part, that act authorized GAO access to the tax returns and return information available to agencies other than IRS or the Bureau of Alcohol, Tobacco and Firearms, but only when GAO is auditing the programs of those agencies for which access to the tax information is authorized by the Internal Revenue Code. In addition, we are reevaluating certain procedures in light of (1) an increased telecommunications capability within GAO, (2) an increased need for GAO to use computers in analyzing tax return information, and (3) our continuing desire to emphasize physical security over tax returns and return information and annual inspection requirements.

After completing our procedural review, we will discuss possible GAO Order 0135.1 revisions with your office. Of course, any procedural change considered will adhere to our general policy that GAO employees are responsible for maintaining control over tax returns and return information and that control should be consistent with IRS Publication 1075 and any additional standards established by IRS.

INTERNAL INSPECTION RESULTS

We accomplish our internal inspection responsibilities through our Group Directors and Evaluators-In-Charge. These individuals share the responsibility for executing our IRS audit assignments, regardless of whether these audits are performed in Washington, D.C., or elsewhere in the country. During the reporting period, the primary GAO offices where staff had access to tax returns and return information were the Washington, D.C., headquarters offices located at 1111 Constitution Avenue N.W., and 1201 "E" Street N.W., and the regional offices located in Atlanta, Chicago, Cincinnati, Dallas, Detroit, Kansas City, Los Angeles, New York, Philadelphia, and San Francisco. Each of these regional offices was visited at least once by GAO Group Directors and/or Evaluators-In-Charge while those audits which involved access to tax return information were being performed.

At headquarters, our Group Directors continuously monitor the implementation of safeguard procedures and adherence to

those procedures by the headquarters staff. Similarly, when making supervisory visits to field offices, the Group Directors and Evaluators-In-Charge review the regional office staff's adherence to GAO Order 0135.1 and IRS Publication 1075. For example, the Group Directors and Evaluators-In-Charge consider whether regional storage and handling of tax returns and return information provide sufficient protection against unauthorized disclosures and whether access to such information is limited to authorized GAO employees. During the continuous monitoring at headquarters and periodic visits to the regional staffs, we detected no systemic tax return or return information safeguard problems or staff deviation from the prescribed procedures.

The following sections of this report, keyed by number to the inspection items enumerated on page 15 of Publication 1075, summarize GAO's procedures for safeguarding tax returns and return information, both at headquarters and in the regions. The following sections also describe any changes made during the reporting period as a result of continuous headquarters monitoring and periodic regional visits.

1. Preventing disclosures through proper storage and handling of tax returns

Security procedures for storing and handling tax returns and return information are needed to assure that employees exercise proper control over the information filed by taxpayers. The procedures must be comprehensive--cover all operational aspects of storing and handling tax returns and return information--and must be designed to prevent unauthorized access to that information.

GAO Order 0135.1 establishes the requisite, comprehensive system for safeguarding the tax returns and return information GAO obtains. In effect, the tax returns and return information are obtained only by authorized GAO headquarters and regional office employees. In general, secure office space and containers for storage of returns and return information are provided by IRS. Only those authorized GAO employees assigned to the audit are given the keys or combinations to the offices or storage containers.

When it is necessary to keep tax return information at the GAO regional or headquarters offices, the information is secured

in cabinets with bars and either combination or key locks, separate from other GAO work, and consistent with IRS procedures. Again, only those employees authorized to work on the assignment are given the combinations or keys to the cabinets. For security purposes, the combinations and key locks are periodically changed and, during off duty hours, the offices are locked. GAO's Office of Security has determined that the regional office sites are configured to meet national security guidelines for the proper storage of classified materials up to and including the secret level.

The following sections, such as those that discuss limiting access to tax returns, securing facilities, commingling tax information, and providing after-hours security, give more detailed information on specific aspects of our procedures and practices for storing and handling tax returns and return information to prevent unauthorized disclosures.

2. Preventing disclosures by limiting access to tax returns

To assure the confidentiality of the information filed by taxpayers, access to this information must be limited to only those employees having a need to know.

GAO procedures are sufficiently detailed to assure that only employees needing access to tax returns and return information can, in fact, gain access to that information. Every 6 months the Comptroller General, after evaluation of both staffing and workload plans by the appropriate GAO managers, designates in writing the name and title of each officer and employee of GAO whose duties require access to tax returns and return information for the purpose of carrying out audits authorized by the Internal Revenue Code. Certified copies of the lists of officers and employees authorized access are delivered to the Committee on Ways and Means and the Committee on Government Operations, House of Representatives; the Committee on Finance and the Committee on Governmental Affairs, U.S. Senate; the Joint Committee on Taxation; the Commissioner of IRS; and, when appropriate, the Director of the Bureau of Alcohol, Tobacco and Firearms or any other agency maintaining tax records. Each month, GAO managers review and amend the lists to account for any assignment and staffing changes. Copies of the amended lists are then provided to the appropriate recipients.

Our review of the procedures followed for authorizing employee access to tax returns and return information showed no systemic problems. Furthermore, we believe that the 6-month period for evaluating the overall need for GAO staff access to tax return information, coupled with monthly updates to account for any personnel changes, is an appropriate and effective means for controlling access to such information.

3. Preventing disclosures through facility security

Adequate facility security is necessary to prevent unauthorized access to the areas in which tax returns and return information are stored. In most instances, IRS is responsible for providing GAO with adequate facility security.

Because GAO stores tax returns and return information in IRS-controlled facilities, the primary responsibility for facility security resides with IRS. For example, tax return information obtained by GAO's headquarters Tax Group is stored in IRS-controlled facilities located at 1111 Constitution Avenue, N.W., and 1201 "E" Street, N.W., Washington, D.C. Similarly, GAO regional office personnel also generally store and have access to returns and return information within IRS-controlled facilities, such as IRS district offices or service centers which have been selected as part of the scope of a GAO audit. In most instances, the information is kept at these IRS facilities until the working papers are transferred to the Tax Group located in IRS-controlled facilities in Washington, D.C. Such transfers are made in accordance with applicable safeguard procedures. These procedures require the use of registered mail with the return receipt signed by a designated employee authorized access to tax return information.

In the few instances that tax returns and return information are kept in non-IRS buildings occupied by GAO, the facility security features are sufficient to prevent unauthorized access to the areas in which tax returns and return information are stored. Specifically, during the conduct of an audit assignment, working papers containing tax returns and return information may be stored at one or more GAO regional offices. The regional offices are housed in GSA-controlled buildings each having GSA-provided security. Furthermore, the primary regional offices identified on page 2 have been inspected by GAO's Office of Security and Safety--the GAO office responsible for facility security--and have been determined to meet national

security guidelines for the proper storage of classified materials up to and including the secret level. Accordingly, we have no safeguard problems attributable to facility security features.

4. Preventing disclosure by not commingling tax and nontax records

To further assure that the confidentiality of taxpayer information is protected from an inadvertent disclosure, tax returns and return information should not be commingled with general agency records. Such commingling is prevented by GAO's (1) standard operating procedures for controlling and disposing of working papers and (2) procedures for disposing of working papers containing tax return information.

In accordance with standard GAO operating procedures, the information obtained during each GAO audit assignment is kept separate from both the agency's general records and other audit assignments. Regardless of whether access to tax returns or return information is involved, the information accumulated during an audit assignment is compiled in working paper bundles, controlled officewide by an assignment authorization number, secured in locked cabinets, and filed separately from other office records. On completion of an assignment and determination that the working papers are not required "onsite," the entire file of working papers is shipped to a federal records center for storage in controlled space. Again, these records are controlled by the officewide assignment authorization number.

GAO's procedures for disposing of working papers containing tax returns and return information further guarantee that tax information will not be commingled with general agency records. In accordance with GAO Order 0135.1, original tax returns are returned to IRS, while the remaining working paper files are shipped to that section of the federal records center IRS uses to store tax returns or return information. Under certain conditions, the working paper files are shredded by GAO staff authorized access to tax return information. Further details on the disposal of tax returns and return information are provided under item 13.

Our analysis of recent disposal records showed that the procedures discussed above have been followed. Moreover, we found no unauthorized disposals nor potential for commingling of tax information with GAO's general records.

5. Preventing disclosures through after-hours security

Adequate after-hours security is necessary to prevent unauthorized individuals from gaining access to the areas where tax returns and return information are stored. As discussed under facility security features, IRS has the primary responsibility for providing security because our work is performed principally in IRS-controlled facilities. For that information stored at GAO regional offices, the GAO Office of Security has determined that security is sufficient to meet national security guidelines for the proper storage of classified materials up to and including the secret level. Consequently, we have no systemic safeguard problems attributable to after-hours security features.

6. Preventing disclosures by limiting access to storage containers

To prevent unauthorized access to tax returns and return information stored in locked containers or safes, the lock combinations and keys should be provided only to those authorized employees who have a need to access the information stored in the containers. Further, the lock combinations should be changed at least annually to assure that only currently authorized employees gain access to the storage containers.

Our review of the procedures followed by GAO headquarters and regional offices in storing, handling, and authorizing access to tax returns and return information--see items 1, 2, and 4--showed no systemic problems. However, in focusing our review on the procedures for authorizing access to the individual locked containers used by the various groups, we identified and immediately corrected one potential safeguard problem. Our review of our records showed that lock combinations had not been changed in over a year. Therefore, combination change orders were submitted to the GAO locksmith who promptly altered all the combinations. Furthermore, arrangements were made to have the combinations changed on an annual basis.

7. Preventing disclosures by analyzing security procedures

Another phase in safeguarding tax returns and return information is to take the steps necessary to assure that security procedures are appropriate for current operations and are

clearly presented to employees. Accordingly, existing procedures should be reviewed in light of any operational changes that may have occurred because of workload or authorizing statute modifications. This review should also assess the adequacy of the safeguard instructions given to employees.

As discussed in the section "Changes To Safeguard Procedures," we are currently reviewing our procedures for safeguarding tax returns and return information. We are making this review because of changes to our access authority stemming from the 1982 Tax Equity and Fiscal Responsibility Act. Also, we are evaluating our procedures in light of an increased telecommunications capability within GAO, an increased need for GAO to use computers in analyzing tax return information, and our continuing desire to emphasize physical security over tax return information and annual inspection requirements.

Until our review is completed, we will continue to provide copies of the existing GAO Order 0135.1 and IRS Publication 1075, Tax Information Security Guidelines, to all GAO employees who need to access tax return information. These procedures have proven to be effective in preventing unauthorized disclosures of this information. The GAO order clearly specifies that employees are responsible for maintaining control over tax returns and return information as well as complying with all applicable IRS standards.

In accordance with GAO's standard operating procedures, any changes adopted from our review will be transmitted to all GAO headquarters and regional employees who have a need to access tax returns and return information. These actions should further heighten employee awareness of tax return information security procedures.

8. Preventing disclosures through controls on automatic data processing operations

To prevent the disclosure of tax return information during computer processing operations, Publication 1075 establishes security requirements for limiting access to information stored on magnetic media. For example, while tax data remains in computer memory, access to the computer must be limited to authorized personnel. Also, tax data cannot remain on any accessible computer storage component after the computer operation has been carried out.

To best assure adherence to the security requirements, we have revised our computer processing practices so that we now rely almost completely on IRS' computer systems. Instead of repeatedly negotiating with other agencies for secure systems to process tax return information--GAO does not presently have its own computer facility--we are now using IRS' National Computer Center through remote access from the IRS national office. Also, other computer processing is performed at IRS service centers on an as available basis. Accordingly, responsibility for assuring a secure system resides with the agency most familiar with the processing requirements for safeguarding tax return information--IRS.

From time to time, however, GAO may have to obtain computer support from sources other than IRS. In those instances, our procedures require GAO employees to control the return information in accordance with IRS' security requirements. In addition, GAO procedures specify that when working in non-IRS facilities:

--all processing phases shall be monitored by an onsite GAO employee authorized access to tax return information;

--all output resulting from processing shall be received by a GAO employee authorized access to tax return information;

--all files, reports, and related items shall be secured before and after processing by a GAO employee authorized access to tax return information; and

--all tax information shall be removed from the computer's memory at the end of processing.

These procedures should ensure the security of tax return information if computer processing at non-IRS facilities becomes necessary.

9. Preventing disclosures through the control and storage of magnetic tapes

To prevent unauthorized access of magnetic tape files containing tax return information, these files must be kept in a secured area and controlled in a manner similar to tax returns. With the change in practice concerning our automatic data processing operations, our computer processing of tax return

information has been performed within IRS facilities. Accordingly, IRS is primarily responsible for the control and storage of magnetic tapes. In those instances when magnetic tapes are retained by GAO after computer processing, the tapes are kept in locked cabinets until they are electromagnetically erased in accordance with Publication 1075 requirements. The same procedures would apply to GAO's processing of tax return information at non-IRS facilities if such computer processing proves necessary.

10. Preventing disclosures through controls on centralized file room activities

GAO does not maintain a centralized file room. Consequently, this inspection requirement, as established by Publication 1075, does not apply to our operations.

11. Preventing disclosures through verification of employee security awareness

Because the security of taxpayer information depends on individual employee action, it is necessary to verify employee awareness of responsibilities for safeguarding tax returns and return information.

Through discussions with GAO headquarters and field personnel responsible for audit assignments involving tax return information, we verified that these employees are keenly aware of their responsibility for safeguarding such information. We attribute this awareness primarily to the safeguard briefings we give new employees and the subsequent reinforcement provided during conferences held at the beginning of each audit assignment. At these briefings and conferences, both GAO Order 0135.1 and IRS Publication 1075 are discussed. These documents clearly describe employee responsibilities for maintaining control over the tax returns and return information.

12. Preventing disclosures by accounting for planned organizational changes

We do not anticipate organizational changes during the next reporting period. Therefore, the requirement for reviewing planned organizational changes to assure that security considerations are covered does not apply at this time.

13. Preventing disclosures by following appropriate disposal procedures

When tax returns and return information are no longer needed, authorized recipients must use disposal procedures which protect the confidentiality of the records. In part, GAO fulfills this responsibility by returning original tax returns obtained during an assignment to IRS for appropriate safeguarding and disposal. Furthermore, GAO's procedures for disposing of copies of tax returns not returned to IRS, as well as other tax return information maintained by GAO, are sufficient to prevent unauthorized disclosures of this information.

Periodically, GAO management evaluates whether working paper files on completed assignments should be disposed of or stored at a federal records center. These working paper files, including copies of tax returns and return information, are stored in locked cabinets at the two IRS facilities located in Washington, D.C.--1201 "E" St. N.W., and 1111 Constitution Ave. N.W. When those tax returns, return information, and related working papers are no longer needed, they are either shredded or sent to the Washington National Records Center. Detailed records on the disposals are maintained by the Tax Group.

When return information is shredded, it is done under the control of a GAO employee who is authorized access to tax returns and return information. Prior to the destruction of the information, the employee is informed of the procedures specified in Publication 1075.

When return information is sent to the records center, shipping and storage instructions specify that storage and subsequent destruction is to be performed at the same level of protection as IRS documents and that access is to be limited to those GAO employees who are specifically authorized access to such information. The instructions further specify that confirmation of names should be obtained by calling the listed phone number of the GAO Tax Group at the IRS National Office.

Our review of the Tax Group's recent information disposal records showed no unauthorized disposals or indications that disposal procedures should be changed.

IDENTIFICATION OF
RETURN INFORMATION DISPOSALS

In accordance with the previously described safeguard procedures, over the period January 1, 1982, through December 31, 1983, GAO transferred 42 boxes containing copies of tax returns, return information, and related working papers to the Washington National Records Center. A list of the items transferred follows.

Assignment authorization code	Number of boxes	Date of transfer
268089	16	11/10/82
268023	3	11/10/82
268050	1	11/10/82
268046	5	11/10/82
268014	1	11/10/82
268027	1	11/10/82
268060	2	11/10/82
268073	1	11/10/82
268044	2	11/10/82
268056	2	11/10/82
268055	2	11/10/82
268074	6	11/10/82
Total	42	

In addition, on October 14, 1983, the working paper files, including associated copies of tax returns and return information, from the following three audit assignments were shredded:

--review of IRS' Post Audit Review Activities (assignment authorization code 268028);

--review of IRS' Efforts to Detect Individual Nonfilers and Secure Delinquent Returns (assignment authorization code 268051); and

--survey of ATF's Tax Administration Activities (assignment authorization code 268058).

In accordance with established procedures, the shredding was done under the control of a GAO employee authorized access to tax returns and return information.

- - - -

As detailed by this report, our review of the procedures followed by both GAO headquarters and regional staff disclosed no systemic safeguard problems requiring procedural change. Nevertheless, adequately safeguarding tax returns and return information will continue to be a major concern to GAO officials and employees. In this regard, I look forward to continuing the effective and cooperative working relationship that exists between your staff and ours in attempting to identify the best measures practicable to assure that taxpayer rights to privacy are safeguarded. If you have questions about any of our safeguarding activities, please contact me on FTS 275-6407.

In accordance with Publication 1075, we are also sending a copy of this report to the Baltimore District Office Disclosure Officer.

Sincerely yours,

Johnny C. Finch

Johnny C. Finch
Senior Associate Director