United States General Accounting Office

GAO

Report to the Honorable Paul Coverdell
U. S. Senate

March 1999

CONFIDENTIALITY OF TAX DATA

IRS' Implementation of the Taxpayer Browsing Protection Act

GAO/GGD-99-43

GAO

United States
General Accounting Office
Washington, D.C. 20548

General Government Division

B-281988

March 31, 1999

The Honorable Paul Coverdell
United States Senate

Dear Senator Coverdell:

This report responds to your request that we determine what the Internal Revenue Service (IRS) has done to implement the Taxpayer Browsing Protection Act (Public Law 105-35).[1] That law, which was enacted on August 5, 1997, made willful unauthorized inspection of taxpayer data illegal. As agreed with your office, this report discusses (1) actions IRS has taken to implement the law and (2) the number of potential and proven incidents of unauthorized access by IRS employees[2] that IRS has identified since enactment of the law, as well as the penalties imposed in cases where unauthorized access was proven.

Results in Brief

IRS has two approaches for implementing P.L. 105-35. Over the long term, IRS believes that modernizing its core automated systems offers the best means to prevent and detect unauthorized access to taxpayer data. According to IRS, modernization will (1) allow it to restrict employees' access to only those taxpayer records that they have a specific work-related reason to look at and (2) enable it to detect unauthorized accesses almost as soon as they happen. It will be several years, however, before this modernization becomes a reality.

In the meantime, IRS has taken several other steps directed at deterring, preventing, and detecting unauthorized access and ensuring that consistent disciplinary action is taken when unauthorized access is proven. For example, IRS

- provides agencywide briefings to all employees on unauthorized access and has developed a form to be signed by all employees to document attendance at a briefing and receipt of guidance on what constitutes an unauthorized access;

[1] P. L. 105-35, 111 Stat. 1104 (1997).

[2] Instead of "browsing," IRS uses the acronym "UNAX" to cover all cases of willful unauthorized access or inspection of taxpayer records. In this report, we use "unauthorized access" instead of UNAX.

- centralized within the Office of the Chief Inspector the identification and investigation of potential access violations;[3]
- created a Centralized Adjudication Unit (CAU) in the National Office to track proven access violations and to provide assistance in administering penalties; and
- implemented an automated tool that is expected to improve IRS' ability to detect unauthorized accesses.

Between October 1, 1997, and November 30, 1998, the Office of the Chief Inspector identified 5,468 potential instances of unauthorized access (i.e., "leads") and completed preliminary investigative work on 4,392 of those leads.[4] Of those 4,392 leads, 338 were determined to warrant further investigation. Many of these 338 cases were still under investigation or in the process of adjudication as of January 25, 1999. Using data provided by IRS, we identified 36 cases for which investigation and adjudication had been completed. Of those 36 cases, 15 involved an IRS determination that IRS employees had intentionally accessed taxpayer data without authorization. In the other 21 cases, IRS determined that either there was no unauthorized access or the access was accidental.

According to IRS, employees involved in the 15 cases of intentional unauthorized access either resigned in lieu of termination or were terminated. According to IRS data, proven cases of unauthorized access that occurred after enactment of Public Law 105-35 have generally been referred to U.S. Attorneys for prosecution, and these U.S. Attorneys have, with one exception, declined to prosecute. According to IRS, the one case that was accepted for prosecution was still open as of February 2, 1999, but the employee has been removed from the agency.[5] As required by the law, IRS notified the three taxpayers whose data the employee had accessed.

[3]In January 1999, after we had completed our audit work, most of the activities of the Office of the Chief Inspector, including those discussed in this report, were transferred to the Treasury Inspector General for Tax Administration—a new position established by the IRS Restructuring and Reform Act of 1998. Because that transfer occurred after we completed our audit work, we refer to the Office of the Chief Inspector in this report.

[4]October 1, 1997, is the starting date for these statistics rather than August 5, 1997 (the date the law was enacted), because the centralized unit responsible for identifying potential cases of unauthorized access was created on October 1, 1997.

[5]Because this case was still open as of February 2, 1999, it is not one of the 15 cases discussed earlier in which intentional unauthorized access was proven.

Background

Over the past few years, both IRS' Office of Internal Audit and we have reported on the need for improved controls to protect against unauthorized accesses of taxpayer data by IRS employees.

In October 1992, Internal Audit reported that IRS had limited ability to prevent unauthorized accesses and detect such accesses once they had occurred.[6] In September 1993, we reported that IRS did not adequately monitor the activities of thousands of employees who were authorized to read and change taxpayer files.[7] We noted that the greatest risk involved IRS' Integrated Data Retrieval System (IDRS), which is the primary computer system used by IRS employees to access and adjust taxpayer accounts.[8] In 1994, IRS implemented an automated tool—the Electronic Audit Research Log (EARL)—to monitor and detect unauthorized accesses to data on IDRS.

In August 1995, we reported that IRS had taken some actions to, among other things, restrict account access and analyze computer usage.[9] We concluded, however, that IRS still lacked sufficient safeguards to prevent or detect unauthorized accesses of taxpayer information. We noted, for example, that security reports issued to monitor and identify unauthorized accesses were cumbersome and virtually useless to managers responsible for ensuring computer security. In 1996, IRS implemented enhancements to EARL that were designed to improve the quality of data being provided to managers. In April 1997, we reported on continuing shortcomings in IRS' efforts to prevent unauthorized access to confidential taxpayer data.[10] We noted, for example, that IRS did not (1) monitor all employees with access to automated systems and data for evidence of unauthorized access, (2) consistently investigate cases involving unauthorized access, and (3) consistently discipline employees who accessed taxpayer data without authorization.

[6]Review of Controls over IDRS Security, IRS Internal Audit Reference No. 030103, October 23, 1992.

[7]IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, Sept. 22, 1993).

[8]IRS officials estimated that about 85 percent of all taxpayer accesses are made through IDRS. The remaining 15 percent are made through other IRS systems.

[9]Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/AIMD-95-141, Aug. 4, 1995).

[10]IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, Apr. 8, 1997).

Because of continuing concerns about unauthorized accesses, Public Law 105-35 was signed into law on August 5, 1997. The law made willful unauthorized inspection of taxpayer data illegal. The law provides that a person convicted of unauthorized access shall be subject to a fine of up to $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution. The law also states that an officer or employee of the United States who is convicted of any such violation shall, in addition to any other punishment, be dismissed from office or discharged from employment. In cases where a person is criminally charged with unauthorized access, the law requires that the Secretary of the Treasury notify the taxpayer whose tax information was accessed.

Scope and Methodology

To achieve our objectives, we

- interviewed officials from IRS' Centralized Case Development Center (CCDC), CAU, Office of Systems Standards and Evaluation, and Office of Chief Inspector (we discuss the role of each of these offices later in the report);
- visited the CCDC in Cincinnati, OH, to observe its operations;
- analyzed data runs that IRS produced at our request as well as IRS management information system reports on unauthorized access; and
- reviewed IRS reports and documentation on unauthorized access.

Other than checking for consistency, we did not verify the reliability of statistical data provided by IRS. We also did not assess the effectiveness of the various actions taken by IRS since enactment of Public Law 105-35.

We requested comments on a draft of this report from IRS and the Acting Treasury Inspector General for Tax Administration. Their comments are discussed near the end of this letter. We did our work from October 1998 through January 1999 in accordance with generally accepted government auditing standards.

IRS' Actions to Implement Public Law 105-35

In an August 1997 report on controlling unauthorized access to taxpayer records, IRS concluded that, in the long run, the best solution was to modernize core IRS systems. According to IRS, modernization will (1) allow it to restrict employees' access to only those taxpayer records that they have a specific work-related reason to look at and (2) enable it to detect unauthorized accesses almost as soon as they happen. However, IRS does not expect to implement those modernization efforts for several years. In the meantime, IRS has taken several steps directed at deterring, preventing, and detecting unauthorized access and ensuring that

appropriate disciplinary action is taken when unauthorized access is proven.

Steps Taken by IRS to Deter Unauthorized Access

Some of IRS' actions are intended to deter unauthorized access (i.e., keep employees from trying to access taxpayer data without authorization). These actions focus on awareness. In an attempt to make certain that all employees are explicitly informed about unauthorized access and the related penalties, IRS, among other things,

- adopted a policy that proven instances of unauthorized access will result in removal from IRS, absent any extenuating circumstances;
- sent a memo in October 1997 to all IRS employees that discussed, among other things, the penalties associated with unauthorized access;
- started giving annual agencywide briefings in November 1997 to inform all employees of IRS' unauthorized access policy and the penalties for violations;
- created a form that is to be signed by employees and managers to acknowledge attendance at a briefing and receipt of guides on what constitutes unauthorized access;
- created a policy that all employees who join or return to IRS after the annual awareness briefings have been administered will be given their briefing within 30 days;
- developed a standard message to be given in all training courses in which access to tax information is discussed;
- developed a video and guides on unauthorized access to ensure that managers deliver a consistent message in briefing employees; and finally,
- established an unauthorized access steering committee and unauthorized access support team to address questions and issues raised by employees and managers.

Steps Taken by IRS to Prevent Unauthorized Access

Other IRS actions are intended to prevent unauthorized access (i.e., stop employees who intentionally or unintentionally try to access taxpayer data without authorization). In that regard, according to IRS, the most effective way to safeguard against unauthorized access is to build controls into automated systems that prevent employees from accessing information they have no need to access. However, according to IRS, its current systems cannot be effectively modified to provide the "need to know" environment that allows employees to access taxpayers' records only when they have a work-related reason to do so. IRS expects to correct this situation as part of its long-term systems modernization effort. In the meantime, IRS has taken some steps to prevent unauthorized access. For example, IRS (1) has incorporated blocks into its systems to prevent employees from accessing their own records and, in some cases, the

records of their spouses or ex-spouses and (2) is reviewing the access rights given to individual employees to ensure that they do not have greater access to tax data than is necessary to do their work.

Steps Taken by IRS to Detect Unauthorized Accesses to Taxpayer Data on IDRS

Until February 1999, when a new system was implemented, IRS depended primarily on EARL to identify potential instances of unauthorized access through after-the-fact analysis of accesses to data on IDRS. EARL used data analysis techniques based on a few known patterns of abuse to identify potential cases of unauthorized access. When EARL was run, it created lists of potential violations (leads) that were provided to analysts at each of IRS' 10 service centers. The analysts were responsible for researching the lists to determine whether the leads warranted further investigation. An IRS study done in August 1997 concluded that the just-described process did not provide the consistent approach needed to support IRS' policy on unauthorized access of taxpayer records. According to the study report and IRS officials, (1) there was a lack of uniformity in the output produced by EARL because each service center had developed its own computer programs, (2) most EARL leads required labor-intensive research to determine whether unauthorized access likely took place, and (3) each service center had developed its own techniques for developing EARL cases.

To correct this lack of a consistent approach to unauthorized access, IRS (1) centralized responsibility for identifying and investigating potential instances of unauthorized access in CCDC, which is located within IRS' Office of the Chief Inspector, and (2) developed a new automated tool to provide better unauthorized access detection capabilities.

Creation of CCDC

In May 1997, the Acting Commissioner of Internal Revenue transferred responsibility for the detection of unauthorized access to the Office of the Chief Inspector. In October 1997, the Chief Inspector created CCDC, which is responsible for identifying potential cases of unauthorized access and determining whether they warrant further investigation by the Internal Security Division in the Office of the Chief Inspector. CCDC became operational in February 1998, when it began assuming responsibility from the 10 service centers for analyzing unauthorized access leads. The transition was completed in September 1998. Since then, CCDC has been responsible for reviewing all leads and deciding which, if any, should be referred to Internal Security. The CCDC staff includes forensic data analysts, security analysts, computer programmers, and criminal investigators. In addition to referrals from CCDC, Internal Security also receives allegations of unauthorized access from various other sources,

such as calls to the Inspection Service integrity hotline from IRS employees, taxpayers, and tax practitioners.

Implementation of New Automated Tool

IRS, in February 1999, implemented the Audit Trail Lead Analysis System (ATLAS) to replace EARL. IRS officials stated that ATLAS is an improvement over EARL because ATLAS (1) will provide better unauthorized access detection capabilities and (2) is a national system that will not be subject to local modifications and practices by the 10 service centers. These improvements, according to the Director of CCDC and IRS documents, will produce better leads than those produced by EARL, because they are more indicative of potential unauthorized access.

For example, according to IRS, ATLAS is programmed to do an exact match between an employee's name and the names of taxpayers whose tax information the employee has accessed. EARL's name match component, on the other hand, only matched the first six characters of the last names. According to IRS data, of the 5,468 total leads received by the Office of the Chief Inspector between October 1, 1997, and November 30, 1998, EARL's match of the first six characters of an employee's name accounted for 3,793 (69.4 percent). However, of the 338 closed leads that were referred to Internal Security for investigation, only 67 (19.8 percent) were generated by EARL's name match. According to the Director of CCDC and IRS documents, ATLAS' increased precision in matching names should result in fewer leads—because there will now have to be an exact match of last names—but these should be more indicative of potential unauthorized access.

Steps Taken by IRS to Detect Unauthorized Access to Taxpayer Data on Systems Other Than IDRS

Although IRS has taken several steps to identify unauthorized accesses involving IDRS, it has done little to detect accesses involving the estimated 130 other information systems that contain taxpayer information. IRS does not have a system such as EARL or ATLAS to analyze accesses involving these other systems. IRS officials in the Systems Standards and Evaluation Office (the office with overall responsibility for security and privacy within IRS) informed us that this problem is to be corrected as part of IRS' long-term systems modernization efforts. However, these efforts will not be implemented for several years. Meanwhile, according to these officials, they have been looking at the controls in these various information systems to prevent unauthorized access. They also said that they depend on the supervisors of employees who use non-IDRS information systems to be on the alert for unauthorized access.

Steps Taken by IRS to Ensure Consistent Disciplinary Actions

In August 1997, the Office of Systems Standards and Evaluation reported that the handling and tracking of unauthorized access cases had not been consistent. The report further stated that IRS would be better served if key operations were centralized to establish consistency and timeliness in developing cases, making decisions on levels of evidence for removals and legal actions, processing and implementing removals, and tracking and reporting cases.

To deal with inconsistencies in case handling and tracking, IRS created CAU within the Labor Relations Office in the National Office. CAU, which became operational in October 1997, is responsible for tracking and reporting the status of all unauthorized access cases; preparing paperwork for all cases, including those in which unauthorized access was not proven;[11] forwarding paperwork on cases to the heads of the appropriate offices for clearance or disciplinary action; and providing consultative support to management in the administration of discipline. To further ensure that consistent disciplinary actions are imposed for proven cases of unauthorized access, the Systems Standards and Evaluation Office is tasked with reviewing those actions.

Number of Potential and Proven Instances of Unauthorized Access and the Penalties Imposed

Between October 1, 1997, and November 30, 1998, the Office of the Chief Inspector received 5,468 leads (information indicating potential unauthorized accesses) and completed work on 4,392 of those leads.[12] Of the 4,392 closed leads, 338 (8 percent) resulted in referrals to Internal Security. Table 1 shows the disposition of the 4,054 closed leads not referred for investigation.

Table 1: Disposition of Closed Leads Not Referred for Investigation Disposition

Disposition	Number
Resolved—access business related	2,493
No basis for referral—further research not warranted[a]	1,446
Cancelled—lead entered in error[b]	115
Total	**4,054**

[a]According to IRS, this disposition category was used when (1) the EARL lead was invalid and there was no reason for the lead to have been identified by the system or (2) research on the lead could not develop information to substantiate either a business-related or a nonbusiness-related connection between the employee and the taxpayer whose data was accessed.

[b]According to IRS, this disposition category was used when the lead was entered in error, such as the wrong employee SSN, or when it was a duplicate to a lead that was already open in the system.

Source: GAO analysis of data obtained from CCDC on the disposition of leads closed by the Office of the Chief Inspector between October 1, 1997, and November 30, 1998.

[11]According to IRS, any case in which the employee was interviewed during the investigation must be forwarded to CAU.

[12]October 1, 1997, is the starting date for statistics in this section, rather than August 5, 1997 (the date the law was enacted), because CCDC was created on October 1, 1997.

During the period covered by our review, EARL accounted for a large majority of the leads received by the Office of the Chief Inspector and most of the cases referred to Internal Security for further investigation. Of the 5,468 leads received by the Chief Inspector during the 14 months ending November 30, 1998, 4,742, or 87 percent, were generated by EARL.[13] The other 13 percent came from other sources, such as complaints from taxpayers and IRS employees. Although most of the leads referred to Internal Security also came from EARL (about 56 percent of the 338 referrals), other sources of leads proved to be more productive. In that regard, of the EARL leads closed by the Office of the Chief Inspector, 5 percent were referred for investigation compared with about 22 percent of the leads from other sources.

Between October 1, 1997, and November 30, 1998, according to IRS' data, Internal Security opened at least 139 investigations[14] of cases in which unauthorized access was alleged to have occurred after passage of Public Law 105-35.[15] As of November 30, 1998, Internal Security had completed 86 of these investigations, while the other 53 investigations were still ongoing.[16]

From October 1, 1997, to January 25, 1999, according to IRS, Internal Security sent CAU 64 cases for adjudication in which unauthorized access was alleged to have taken place after enactment of Public Law 105-35.[17] As of January 25, 1999, action had been completed on 36 of these cases, and 28 remained open. In 15 of the 36 completed cases, IRS determined that an intentional unauthorized access had occurred. Of the remaining 21 cases, IRS determined that 14 involved no unauthorized access, 6 involved accidental accesses that were reported by the employees to their

[13]As discussed earlier, of the leads generated by EARL, 3,793 resulted from EARL's name match component.

[14]We say "at least" because there were gaps in IRS' data that prevented us from knowing in all cases whether an opened investigation involved an access that occurred after passage of Public Law 105-35. If we could not tell when the access occurred, we did not include the investigation in our count of 139. There were 80 cases for which we could not determine the date of the alleged unauthorized access.

[15]The 139 opened investigations cannot be related back to the 338 referrals from CCDC discussed earlier because, as noted earlier, Internal Security receives allegations of unauthorized access from sources other than CCDC.

[16]During this time, Internal Security was also investigating unauthorized accesses that were alleged to have taken place before passage of Public Law 105-35.

[17]The number of cases received for adjudication (64) could differ from the number of investigations completed by Internal Security (86) because not all completed investigations require adjudication. If Internal Security determines, as a result of its investigation, that there was no unauthorized access and if the employee was not interviewed as part of the investigation, the case need not be sent to CAU.

supervisors in accordance with established procedures, and 1 involved an accidental access that was not reported in accordance with established procedures. In the latter case, the employee was reprimanded.

As shown in table 2, of the 15 proven intentional unauthorized accesses, 10 involved service center employees, and 5 involved district office employees. According to IRS, the offending employees in those 15 cases either resigned in lieu of termination or were terminated.[18]

Table 2: Number of Intentional Unauthorized Accesses by IRS Location

Location	Number of unauthorized accesses
Service center	
Andover	2
Brookhaven	2
Atlanta	1
Austin	1
Kansas City	1
Memphis	1
Ogden	1
Philadelphia	1
Subtotal	**10**
District office	
Ohio	2
Gulf Coast	1
Indianapolis	1
New Jersey	1
Subtotal	**5**
Total	**15**

Source: Data obtained from CAU on cases completed between October 1,1997, and January 25, 1999, in which IRS had determined that an intentional unauthorized access had occurred after enactment of Public Law 105-35.

According to IRS data, proven cases of unauthorized access that occurred after enactment of Public Law 105-35 have generally been referred to U.S. Attorneys for possible prosecution. In almost every case, according to IRS data, the U.S. Attorney declined to prosecute. As of February 2, 1999, one case had been accepted for prosecution.[19] According to IRS, although the case was still open, the employee had been removed from the agency. Pursuant to the law, IRS notified the three taxpayers whose data the employee had accessed.

[18]As of January 25, 1999, CAU also had 11 open cases in which removal of the employee had been proposed and 5 cases in which it was preparing a removal proposal.

[19]This case is in addition to the 15 cases discussed earlier in which intentional unauthorized access was proven. Because legal action had not yet been completed, this case was considered one of the 28 cases that were open as of January 25, 1999.

Agency Comments

We obtained written comments on a draft of this report from IRS' Chief Information Officer (see app. I) and the Acting Treasury Inspector General for Tax Administration (see app. II).

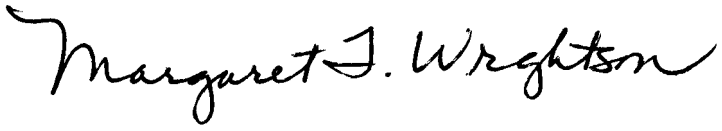
The Chief Information Officer said that IRS agreed with the information in our report. He emphasized that, in some regards, IRS' current weaknesses are associated with its aging systems and that these weaknesses will be corrected as part of IRS' long-term systems modernization plans. In the meantime, according to the Chief Information Officer, IRS (1) has initiated actions to block employees' access to more taxpayer accounts than they are currently restricted from accessing and (2) is reviewing the feasibility of incorporating audit trail records from systems other than IDRS into ATLAS.

The Acting Treasury Inspector General for Tax Administration said that the report provides a good summary of the actions taken by his office (formerly the Office of the Chief Inspector) to implement the provisions of Public Law 105-35. He said that the identification and investigation of unlawful accesses of taxpayer information has been and will remain a high priority of his office.

As agreed with your office, unless you publicly release its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies to Senator William V. Roth, Chairman, and Senator Daniel P. Moynihan, Ranking Minority Member, Senate Committee on Finance; and Representative Bill Archer, Chairman, and Representative Charles B. Rangel, Ranking Minority Member, House Committee on Ways and Means. We will also send copies to the Honorable Robert E. Rubin, Secretary of the Treasury; the Honorable Charles O. Rossotti, Commissioner of Internal Revenue; the Honorable Jacob Lew, Director, Office of Management and Budget; and Mr. Lawrence W. Rogers, Acting Treasury Inspector General for Tax Administration. Copies will be

made available to others upon request. Major contributors to this report were David J. Attianese, Assistant Director; and John Lesser, Evaluator-in-Charge. Please contact me on (202) 512-9110 if you have any questions.

Sincerely yours,



Margaret T. Wrightson
Associate Director, Tax Policy and
Administration Issues

Contents

Abbreviations

ATLAS	Audit Trail Leads Analysis System
CAU	Centralized Adjudication Unit
CCDC	Centralized Case Development Center
EARL	Electronic Audit Research Log
IDRS	Integrated Data Retrieval System
IRS	Internal Revenue Service

Comments From the Internal Revenue Service

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

MAR - 1 1999

Ms. Margaret T. Wrightson
Associate Director, Tax Policy and
Administration Issues
441 G Street, NW
Washington, DC 20548

Dear Ms. Wrightson:

Thank you for the opportunity to comment on your draft report, entitled CONFIDENTIALITY OF TAX DATA: IRS' Implementation of the Taxpayer Browsing Protection Act. It provides a good summarization of actions taken by the IRS to implement the Taxpayer Browsing Protection Act of 1997. In this regard, we agree with the information reported.

An important focus of our program to stop unauthorized access has been in institutionalizing a consistent approach, which includes centralized investigation and adjudication offices. Additionally, the program is aggressively focused on educating all IRS employees on our policy on unauthorized access and inspection of taxpayer records, including the penalties associated with the violation. We believe that these efforts are helping the IRS to mitigate the weaknesses in prevention and detection of unauthorized access. In some regards, our current weaknesses are associated with our aging systems that need to be modernized. As noted in your draft report, the IRS plans to correct these weaknesses, as part of its long-term systems modernization. In the interim, however, we have initiated actions to block access to additional taxpayers. Additionally, we are reviewing the feasibility of migrating audit trail records from more systems to the IRS' new Audit Trail Lead Analysis System.

In closing, thank you again for reporting on the important actions being taken by the IRS to implement the Taxpayer Browsing Protection Act of 1997. Protecting taxpayer records is key to the success of a customer-focused IRS. We look forward to your continuing support and advice in this area.

Sincerely,

Paul J. Cosgrave

Comments From the Acting Treasury Inspector General for Tax Administration

INSPECTOR GENERAL for TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 4, 1999

Ms. Margaret T. Wrightson
Associate Director, Tax Policy and
Administration Issues
General Accounting Office
441 G Street, NW
Washington, D.C. 20548

Dear Ms. Wrightson:

I appreciate having the opportunity to comment on your draft report, entitled "Confidentiality of Tax Data: IRS's Implementation of the Taxpayer Browsing Protection Act". It provides a good summary of the actions taken by the Treasury Inspector General for Tax Administration (TIGTA) (formerly known as the Office of the Chief Inspector) to implement the provisions of the Taxpayer Browsing Act of 1997.

My office remains committed to assisting the IRS by identifying employees who make unauthorized accesses to the accounts of taxpayers. We have assembled a highly trained staff to analyze the leads to identify employees who may improperly access taxpayer accounts. In this analyses we utilize state of the art computer system and programs. Once a potential violation occurs I ensure that the special agents promptly and thoroughly investigate the matter. A report of investigation is then provided to management to determine the appropriate disciplinary for the employee.

Identification and investigation of unlawful accesses of taxpayer information has been and will remain a high priority of TIGTA. Thank you again for the opportunity to comment on your report.

Sincerely,

Lawrence W Rogers

Lawrence W. Rogers
Acting Treasury Inspector General
for Tax Administration

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Order by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touch-tone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested

(268862)